



Ifu

501.43790X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): D. NAKATSUKA

Serial No.: 10/828,287

Filed: April 21, 2004

Title: COMPUTER SYSTEM FOR ALLOCATING STORAGE AREA TO
COMPUTER BASED ON SECURITY LEVEL

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 27, 2004

Sir:

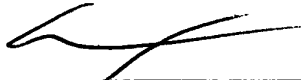
Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby
claim(s) the right of priority based on:

**Japanese Patent Application No. 2004-052700
Filed: February 27, 2004**

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No.: 29,621

CIB/rr
Attachment

CERTIFIED COPY OF
PRIORITY DOCUMENT

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 2 7 日
Date of Application:

出 願 番 号 特 願 2 0 0 4 - 0 5 2 7 0 0
Application Number:
[ST. 10/C]: [J. P 2 0 0 4 - 0 5 2 7 0 0]

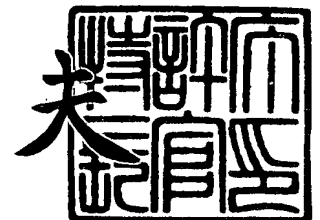
願 人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 4 年 3 月 2 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 2 4 1 8 8

【書類名】 特許願
【整理番号】 K04000211A
【あて先】 特許庁長官殿
【国際特許分類】 G06F 12/00
【発明者】
 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所
 システム開発研究所内
 中塚 大樹
 【氏名】
【特許出願人】
 【識別番号】 000005108
 【氏名又は名称】 株式会社 日立製作所
【代理人】
 【識別番号】 100075096
 【弁理士】
 【氏名又は名称】 作田 康夫
【選任した代理人】
 【識別番号】 100100310
 【弁理士】
 【氏名又は名称】 井上 学
【手数料の表示】
 【予納台帳番号】 013088
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

計算機と、

前記計算機とネットワークを介して接続される記憶装置システムと、

前記計算機及び前記記憶装置システムと接続される第二の計算機とを有し、

前記第二の計算機は、前記記憶装置システムに関する情報を有し、前記計算機の要求に基づいて、前記要求に合致する前記記憶装置システムを前記情報に基づいて選択し、前記選択された記憶装置システムに対して前記計算機が使用する記憶領域を前記計算機の要求に基づいて作成する指示を送信し、

前記記憶装置システムは、前記指示に従って前記計算機の要求を満たす記憶領域を作成し、作成終了を前記第二の計算機へ通知し、

前記第二の計算機は、前記通知の受領後、前記計算機へ前記記憶装置システムで作成された前記記憶領域に対する経路情報を通知することを特徴とする計算機システム。

【請求項 2】

前記記憶装置システムに関する情報とは、前記記憶装置システムのセキュリティレベルに関する情報であり、

前記計算機の要求とは、高いセキュリティレベルが確保される記憶領域の作成の要求であることを特徴とする請求項 1 記載の計算機システム。

【請求項 3】

前記セキュリティレベルに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記高いセキュリティレベルとは、前記装置がIPSec処理を行えるということであることを特徴とする請求項 2 記載の計算機システム。

【請求項 4】

前記指示には、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に前記記憶領域を対応付ける指示であり、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項 3 記載の計算機システム。

【請求項 5】

前記指示は、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える複数の装置に前記記憶領域を対応付ける指示であり、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記複数の装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記複数の装置の個々に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項 3 記載の計算機システム。

【請求項 6】

前記第二の計算機は更に、前記記憶装置システムが有する記憶領域を使用可能な前記ネットワークに接続された前記計算機の情報（以下「第二の情報」）を有し、

前記計算機は、前記第二の計算機に該計算機が使用できる記憶領域の情報の送付要求を発行し、

前記第二の計算機は、前記第二の情報に基づいて、前記計算機が使用できる前記記憶装置システムが有する前記記憶領域への経路情報を前記送付要求を発行した前記計算機に送信することを特徴とする請求項 5 記載の計算機システム。

【請求項 7】

前記第二の計算機は、前記通知の受領後、前記計算機へ前記記憶装置システムで作成された前記記憶領域に対する経路情報を通知する際に、前記記憶領域の作成を要求した前記

計算機についての情報を前記第二の情報に登録することを特徴とする請求項6記載の計算機システム。

【請求項8】

前記記憶装置システムに関する情報とは、前記記憶装置システムのセキュリティレベルに関する情報であり、

前記計算機の要求とは記憶領域の作成の要求であり、

前記第二の計算機は、前記計算機が有するセキュリティレベルに応じて、前記記憶装置システムに前記記憶領域の作成を指示することを特徴とする請求項1記載の計算機システム。

【請求項9】

前記セキュリティレベルに関する情報とは、前記記憶装置システム又は前記計算機が前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記指示には、前記計算機が有するセキュリティレベルが前記IPSec処理を行える装置を有するレベルの場合に、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に前記記憶領域を対応付ける指示であることを特徴とする請求項8記載の計算機システム。

【請求項10】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に対応付けて記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項1記載の計算機システム。

【請求項11】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは、記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える複数の前記装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える複数の前記装置の各々に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項1記載の計算機システム。

【請求項12】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは、記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置及びIPSec処理を行えない前記装置とに対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報及びIPSec処理を行えない

前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項 1 記載の計算記システム。

【請求項 13】

前記計算機は、前記第二の計算機から受信した前記複数のアドレスの情報から一つを選択して前記記憶装置システムが有する前記記憶領域へアクセスすることを特徴とする請求項 11 及び 12 に記載のうちいずれか一つの計算機システム。

【請求項 14】

前記計算機は、該計算機が行う処理が高いセキュリティレベルを必要とする場合には、前記複数のアドレス情報のうち、IPSec処理を行える前記装置に対応するアドレス情報を選択して前記記憶装置システムが有する前記記憶領域へアクセスすることを特徴とする請求項 13 記載の計算機システム。

【請求項 15】

計算機及び記憶装置システムと接続される管理計算機であって、
制御部、メモリ及び前記計算機及び前記記憶装置システムと接続されるネットワークと接続されるインターフェースとを有し、

前記メモリは、ネットワークと接続される前記記憶装置システムが有する装置がIPSec処理を行えるかどうかを示す情報を有し、

前記計算機から前記記憶装置システムにおける記憶領域の作成が前記インターフェースを介して要求された際に、前記制御部は、前記要求に基づいて、IPSec処理を行える装置に対応付けるように前記記憶領域を作成する指示を前記記憶装置システムへ送信し、

前記記憶装置システムから完了通知を受領した後、前記計算機に、前記IPSec処理を行える装置に割り振られたアドレス情報を通知することを特徴とする管理計算機。

【請求項 16】

管理計算機及び記憶装置システムと接続される計算機であって、

制御部、メモリ及び前記管理計算機及び前記記憶装置システムと接続されるネットワークと接続されるインターフェースとを有し、

前記管理計算機へ前記記憶装置システムにおける記憶領域の作成を前記インターフェースを介して要求し、前記制御部は、前記管理計算機から送信された複数のアドレスに関する情報を前記メモリに格納し、

前記複数のアドレスに関する情報から一つを選択して前記記憶装置システムが有する前記記憶領域にアクセスすることを特徴とする計算機。

【請求項 17】

前記計算機及び前記記憶装置システムは複数あることを特徴とする請求項 1 ～ 14 記載の計算機システム。

【請求項 18】

計算機と、

前記計算機とネットワークを介して接続される記憶装置システムと、

前記計算機及び前記記憶装置システムと接続される第二の計算機とを有し、

前記第二の計算機は、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報を有し、前記計算機のIPSec処理を行える前記装置に対応付けられた記憶領域の作成の要求に基づいて、前記要求に合致する前記記憶装置システムを前記情報に基づいて選択し、前記選択された記憶装置システムに対して前記計算機が使用する記憶領域を、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に対応付けて作成する指示を送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、作成終了を前記第二の計算機へ通知し、

前記第二の計算機は、前記計算機に、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知し、

前記計算機は、前記アドレスの情報に基づいて、前記記憶装置システムが有する前記記憶領域に、IPSec処理を行える前記装置を介してアクセスすることを特徴とする計算記シ

● “ ステム。

【書類名】明細書**【発明の名称】**セキュリティレベルに応じて記憶領域を計算機に割り当てるシステム**【技術分野】****【0001】**

本発明は、インターネットプロトコル (IP) ネットワークを用いて複数の計算機や記憶装置システムを結合するストレージエリアネットワーク (以下「IP-SAN」) における記憶領域管理方法に関する。

【背景技術】**【0002】**

企業等でデータを効率よく管理するために、ストレージエリアネットワーク (SAN) が構築されることがある。SANとは複数の記憶装置システムと計算機とを結合するネットワークである。通常SAN内のデータ転送にはファイバチャネル・プロトコル (以下、このSANをFC-SANと言う) が用いられている。

【0003】

一方、近年iSCSIを用いたSANであるIP-SANが注目されている。iSCSIとは、従来計算機と記憶装置システムとの間の通信に用いられていたSCSIコマンド及びそのコマンドに従って転送されるデータを、IPネットワーク経由で送受信するためのプロトコルである。ISCSIについては非特許文献1に詳細が開示されている。IP-SANは、FC-SANに比べ、すでにインフラストラクチャとして利用されている既存のLAN(Local Area Network)機器を活用することができる等の利点がある。

【0004】

しかし、FC-SANとは異なり、IP-SANではインターネットや企業内LANなど、安全性が確保されていないネットワークを使用する場合がある。また、IPネットワークに対しての攻撃方法や攻撃プログラムが広く知れ渡っている。したがって、IP-SANでは、セキュリティに対する配慮が重要である。

【0005】

SANでセキュリティを確保する方法として、計算機と記憶装置システムとの間でのアクセス制限や通信経路の暗号化が考えられる。計算機と記憶装置システムとの間でのアクセス制限技術として、スイッチやファブリックにおいて通信経路を分離するゾーニングや、ポート間においてエンドツウエンドのアクセス制限を行うLUNマスキング(Logical Unit Number マスキング)がある。ここで、LUNマスキングの技術については、例えば特許文献1に開示されている。

【0006】

IP-SANでは、計算機と記憶装置システムとの間の通信経路の暗号化方法としてIPSecを使用することができる。IPSecの詳細については非特許文献2に開示されている。IPSecは共通鍵を用いて通信の暗号化を行う技術である。IPSecでは、共通鍵の管理方式として非特許文献3により規定されるIKE(Internet Key Exchange)が採用されている。

【0007】

【特許文献1】 特開2001-265655号公報 (第2-3項、第1-3図)

【非特許文献1】 Julian Satran等著、「iSCSI」、2003年1月19日、IETF、<URL: <http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt>>

【非特許文献2】 Stephen Kent、Randall Atkinson著、「Security Architecture for IP」、1998年11月、IETF、<URL: <http://www.ietf.org/rfc/rfc2401.txt>>

【非特許文献3】 Dan Harkins、Dave Carrel著、「The Internet Key Exchange (IKE)」、1998年11月、IETF、<URL: <http://www.ietf.org/rfc/rfc2409.txt>>

【発明の開示】**【発明が解決しようとする課題】****【0008】**

IP-SANに接続される装置がすべて上述したセキュリティ確保のための機能を有する訳ではない。例えば、IP-SANに接続される装置には、IPSecが実装されているものとされてい

ないものがある。又、計算機と記憶装置システムとの間の全ての通信においてセキュリティを確保する必要が無い場合もある。

【0009】

このような場合、システム管理者はシステムを構築する際、ネットワークに接続された機器のセキュリティ確保のための機能の有無やシステム内の各部におけるセキュリティレベルを逐次考慮しながら、ネットワークに接続された計算機に、ネットワークに接続された記憶装置システムやその記憶装置システムが有する記憶領域を割り当てる必要がある。これはシステム管理者に過大な負荷がかかる。又、管理者が設定した場合、計算機の利用者が自由にその記憶領域の割当ての設定を変更することが難しい。あるいは、計算機と記憶装置システムとの間の通信で不必要にセキュリティレベルが高い設定がなされ、システムの資源を無駄に使用してしまう。

【課題を解決するための手段】

【0010】

本発明は上記の問題を解決するため、以下の構成を有する。具体的には、ネットワークに接続される計算機や記憶装置システムの情報を管理する計算機（以下「管理計算機」とも言う）を有するシステムとする。そして、管理計算機は、計算機の要求に従って所定の条件を有する記憶装置システムを選択し、その記憶装置システムに対して記憶領域の作成を指示する。指示を受けた記憶装置システムは、指示された条件に従って記憶領域を作成し、管理計算機に作成終了を通知する。

【0011】

通知を受けた管理計算機は、作成された記憶領域を使用するための情報（例えば記憶装置システムが有するポートに振られたネットワークにおけるアドレス等）を計算機に通知する。計算機は通知された情報に基づいて、作成された記憶領域を使用する。

【0012】

ここで、管理計算機が管理する記憶装置システム等の情報とは、セキュリティレベルに関する情報である。又、計算機の要求にはセキュリティレベルに関する要求が含まれていても良い。この場合、管理計算機は、計算機から要求されたセキュリティレベルに合致する記憶装置システムを自身が管理する情報から検索し、その記憶装置システムに対し、記憶領域の作成を指示する。

【0013】

尚、ここでセキュリティレベルとは、各装置においてデータ送受信の暗号化処理が可能かどうかを示す情報でも良い。

【0014】

本発明の他の構成については、実施例等の記載により明らかにされる。

【発明を実施するための最良の形態】

【0015】

図1は、本発明の第一の実施形態におけるシステム構成例を示す図である。システムは、計算機（以下「サーバ」とも言う）101、記憶装置システム102及び管理計算機（以下「管理サーバ」とも言う）103を有する。サーバと記憶装置システムとは、IPネットワーク104で相互に接続されている。また、サーバ、記憶装置システム及び管理サーバは管理用ネットワーク105により相互に接続される。

【0016】

なお、図1に示したシステム構成例ではIPネットワーク104と管理用ネットワーク105をそれぞれ独立したネットワークとして構成しているが、それらを一つのネットワークで共有する構成にしても良い。また、IPネットワーク104に接続されるサーバ101と記憶装置システム102の数は任意である。

【0017】

サーバ101は、IPネットワーク104を介して記憶装置システム102との間でデータの送受信を行う。IPネットワーク104はIPパケットを転送可能なネットワークである。具体的にIPネットワークには、イーサネット（登録商標）により構築されたLANやWAN(W

Local Area Network)、通信事業者により提供される広域IP通信網、専用線等がある。

【0018】

管理サーバ103は、管理用ネットワーク105を介してサーバ101や記憶装置システム102との間で管理情報の送受信を行う。

【0019】

サーバ101は一般的な計算機であり、プロセッサ（以下「CPU」とも言う）106、メモリ107及びホストバスアダプタ（以下「HBA」とも言う）108を有する。CPU106、メモリ107及びHBA108は、バス109を介して相互に接続される。メモリには、バス管理プログラム110、バス情報テーブル111及びパスワード管理テーブル112が格納される。尚、これらのプログラムは、可搬記憶媒体やネットワークを介してサーバ101のメモリ107等に格納される。

【0020】

プロセッサ106は、バス管理プログラム110を実行することで、バス情報テーブル111に格納されているサーバと記憶装置システムとの間の経路情報を元に、IPネットワーク104を介したサーバ101と記憶装置システム102との間のデータ通信経路を決定する。またプロセッサ106は、管理者、ユーザ、他のプログラム等からの情報を元に、データ通信経路の決定や変更を行う。

【0021】

バス情報テーブル111には、サーバ101が、IPネットワーク104に接続される記憶装置システム102へアクセスするために必要な経路情報と、その経路が持つ特性情報（IPSecによる暗号化機能の有無等）が格納される。

【0022】

IPSecを用いてサーバ101と記憶装置システムとの間でデータを暗号化して通信する際には、暗号化に必要な鍵を、通信を行うサーバ101と記憶装置システム102とに設定する必要がある。鍵を設定する鍵管理方法には手動管理方式と自動管理方式がある。ただし、iSCSIの規約では、手動管理方式による鍵管理が禁止されている。また、iSCSI規約では、自動管理方式としてIKE鍵管理プロトコルを実装しなくてはならないと規定している。IKEで鍵交換を行う際、サーバ101と記憶装置システムとの間で相互の認証処理が行われる。パスワード管理テーブル112には、IKEでの認証時に必要となる、装置自身のパスワードが格納される。尚、iSCSI規約に従わなくても良い状況で本発明を使用する場合には、手動管理方式で鍵を設定しても良いし、IKE以外のプロトコルの自動管理方式を採用しても良い。

【0023】

HBA108は、サーバ101とIPネットワーク104とを接続するために用いられる接続機器である。HBA108は、インターフェースチップ（以下「IFチップ」とも言う）113、IPネットワーク104へ接続するための物理ポート115及びIPSec処理部127を有する。サーバ101とIPネットワーク104との間で転送されるデータは、すべてポート115を介して転送される。

【0024】

IFチップ113は、IPネットワーク104へ送受信するパケットの処理（SCSIコマンドのカプセル化等）及び物理ポート115とサーバ101のメモリ107等との間のDMA（Direct Memory Access）転送を制御する回路である。

【0025】

IPSec処理部127は、通信されるデータの暗号化、復号化、装置間の鍵交換及び認証に関する処理等を行うプロセッサである。認証を行う際には、IPSec処理部127は、メモリ107に格納されたパスワード管理テーブル112を検索し、通信相手との認証に必要なパスワードを入手する。

【0026】

尚、本実施形態では、HBA108として、IPSecによる暗号化通信に必要な処理を行えるHBAを仮定した。しかしながら、サーバ101は、実際にはIPSec処理が行えない

HBA108を有する場合もある。以下、これらのHBAを区別する場合、IPSecの処理を行えるHBA108をHBA108aとし、IPSecの処理を行えないHBA108をHBA108bとする。

【0027】

記憶装置システム102は、ホストアダプタ120a、ホストアダプタ120b、CPU116、ディスクアダプタ117、メモリ119、キャッシュメモリ118、ディスクドライブ群121を有する。ホストアダプタ120a、ホストアダプタ120b、CPU116、ディスクアダプタ117、メモリ119及びキャッシュメモリ118は、バス122を介して相互に接続される。バス122の代わりにスイッチが用いられても良い。ディスクアダプタ117は、ディスクドライブ群121とバス122とを相互に接続する。メモリ119には、ボリューム情報テーブル123及びパスワード管理テーブル124が格納される。

【0028】

CPU116は、バス122を介してメモリ119へアクセスし、メモリ119へ格納されたプログラムを実行する。ディスクアダプタ117は、CPU116からディスクドライブ群121へのアクセスの制御を行う。キャッシュメモリ118には、サーバ101へ転送されるデータあるいはサーバ101から転送されてきたデータが一時的に格納される。

【0029】

ディスクドライブ群121は、1つ又は複数のディスクドライブを有する。尚、ディスクドライブ群121は、ディスクドライブのような不揮発性記憶媒体の代わりに、フラッシュメモリカード等の揮発性の記憶媒体を複数有していても良い。個々のディスクドライブは物理的な記憶領域を有する。記憶装置システム102は、個々のディスクドライブが有する物理的な記憶領域から、論理的な記憶領域（以下「物理ボリューム」という）を作成する。この物理ボリュームは、記憶装置システム102が、自身が有する記憶領域を1つの論理的な記憶装置として扱う単位となる。尚、この物理ボリュームを構成するディスクドライブ群がRAID構成であっても良い。

【0030】

さらに記憶装置システム102は、1又は複数の物理ボリュームから、ボリュームを作成する。ボリュームは、サーバ101に対して提供される論理的な記憶領域の一つの単位であり、例えば、SCSI規格で使用する論理ユニット(Logical Unit:LU)に相当する。

【0031】

ホストアダプタ120は、IPネットワーク104と接続される物理ポート125を有する。また、ホストアダプタ120aは、IPSecによる暗号化通信に必要な処理を行うためのIPSec処理部127を有する。本実施形態では、記憶装置システム102がIPSecによる暗号化通信処理を行うホストアダプタ120aとIPSecによる暗号化通信処理を行わないホストアダプタ120bを一つづつ有する構成としたが、記憶装置システム102が有するホストアダプタ120a、bの数は任意である。記憶装置システム102は、ホストアダプタ120aのみ又はbのみを有していても良い。

【0032】

ボリューム情報テーブル123には、物理ボリュームとボリュームとの対応関係を示す情報が格納される。具体的には、ある物理ボリュームに対応するボリュームの番号（以下論理ユニット番号(LUN)と言う）、ボリュームの容量、ボリュームに割り当てられたポート115のID（アドレス等）情報が保持される。記憶装置システム102は、新しいボリュームを作成するたびにボリューム情報テーブル123の内容を更新する。

パスワード管理テーブル124には、記憶装置システム102のホストアダプタ120aがIPSec処理をする際のIKEでの認証時に必要とするパスワードが格納される。

【0033】

管理サーバ103は、一般的な計算機であり、プロセッサ（以下「CPU」とも言う）128、メモリ129、及びネットワーク接続部130を有する。CPU128、メモリ

129、及びネットワーク接続部130は、バス131により相互に接続される。メモリ129には、ネットワーク管理プログラム132及び構成データベース133が格納される。

【0034】

構成データベース133は、ポート情報テーブル134及びストレージ容量管理テーブル135を有する。

ポート情報テーブル134には、管理サーバ103がIPネットワーク104に接続されている物理ポートを管理するための情報が登録される。具体的には、ある物理ポートに対し、その物理ポートを持つ装置を一意に識別する装置ID、その物理ポートへ他の装置がアクセスするためのアドレス、その物理ポートを保持するHBAやホストアダプタがIPSec処理を実行可能か否かの情報が保持される。

【0035】

ストレージ容量管理テーブル135には、管理サーバ103がIPネットワーク104に接続されている記憶装置システム102の記憶容量を管理するための情報が登録される。具体的には、IPネットワーク104に接続される個々の記憶装置システム102が有する記憶領域のうち、まだ使用されていない記憶領域の容量（以下「空き容量」）及び既に使用されている記憶領域の容量（以下「使用済み領域の容量」又は「使用容量」）の情報が、記憶装置システム102毎にストレージ容量管理テーブル135に登録される。

【0036】

管理サーバ103のプロセッサ128は、ネットワーク管理プログラム132を実行して、管理用ネットワーク105を介し、サーバ101や記憶装置システム102がそれぞれ持つ物理ポートの情報、ストレージの空き容量や使用済み領域の容量の情報を収集する。そして、管理サーバ103は、収集した情報に基づいて、ポート情報テーブル134とストレージ容量管理テーブル135を作成したり、更新したりする。

【0037】

また、管理サーバ103は、サーバ101やシステム管理者等からのボリューム作成要求に基づいて、ポート情報テーブル134とストレージ容量管理テーブル135の内容を検索し、条件にあったボリュームの作成要求を記憶装置システム102に対して発行する。更に、ボリューム作成の完了報告を記憶装置システム102から受領した管理サーバ103は、ボリューム作成が完了したことを、ボリューム作成要求を発行したサーバ101や管理者等へ通知する。さらに、管理サーバ103は、IKEを行う際の認証に必要なパスワードを収集し、サーバ101及び記憶装置システム102へ、新たに入力されたパスワードをパスワード管理テーブル112、117へ登録する命令を発行する。

【0038】

以下、各機器が有する各テーブルの内容について説明する。なお、本実施形態では情報はテーブルの形態で管理されているが、情報の管理の仕方はテーブルに限られない。

図2は、ポート情報テーブル134の構成例を示す図である。ポート情報テーブル134は、IPネットワーク104へ接続されている各物理ポート115、125（以下まとめて「物理ポート115等」又は単に「物理ポート」）の特性の情報を保持するテーブルである。

【0039】

ポート情報テーブル134は、IPネットワーク104に接続される物理ポート115等数分のエントリを有する。1つのエントリは、そのエントリに対応する物理ポート115等を有する装置の識別子である装置IDを登録するフィールド201、対応する物理ポート115等へ割り当てられているSCSIオブジェクトのオブジェクトIDを登録するフィールド202、対応する物理ポート115等へ割り当てられているIPアドレスを登録するフィールド203、対応する物理ポート115等を保持する装置がサーバ101であるか記憶装置システム102であることを区分する情報であるノード種別が登録されるフィールド204、対応する物理ポート115等を持つHBA108やホストアダプタ120がIPSec処理部を持つか否かを示す情報が登録されるフィールド205、認証IDが登録される

フィールド 206 及びパスワードを登録するフィールド 207 を有する。

【0040】

ここで物理ポートへのSCSIオブジェクトの割当てとは、サーバ101がSCSIオブジェクトを使用するときに使用する物理ポートを決定することを指す。従って、サーバ101は、他の物理ポートを用いてSCSIオブジェクトを利用することは出来ない。

【0041】

オブジェクトIDとは、SAM (SCSI Architecture Model) にて規定されるSCSIオブジェクトの識別子である。ここでSCSIオブジェクトとは、SCSIコマンドを発行する装置（論理的でも物理的でも良い。以下「SCSIイニシエータ」）と、SCSIコマンドを受信する装置（論理的でも物理的でも良い。以下「SCSIターゲット」）の総称である。オブジェクトIDは、iSCSIではiSCSIネーム、FCではWWNに相当する。IPネットワーク104に接続する装置は1つ以上のSCSIオブジェクトを持つことが可能である。例えば図2に示す例では、装置IDがStorage1である記憶装置システム102はiqn.2003-03.com.example:storage1及びiqn.2003-04.com.example:storage1の2つのSCSIオブジェクト（ここではSCSIターゲット）を保持している。

【0042】

また、物理ポート115等がSCSIオブジェクトへ割り当てられていない場合、フィールド202は空欄になる。例えば、図2に示す例において、装置IDがStorage2である記憶装置システム102の、割り当てIPアドレスが10.10.10.204である物理ポートは、フィールド202が空欄になっている。これは、この物理ポートがSCSIオブジェクトへ割り当てられていないことを示している。

【0043】

認証IDは、IPSecの暗号化処理におけるIKE認証において、鍵交換を行う端末を特定するIDである。認証IDは、IPSecを使用可能な物理ポート毎に割り当てられる。認証IDは、例えば物理ポートに割り当てられているIPアドレス、IPアドレスとネットワークマスクの組又は装置IDなどの名前が使用されても良い。

【0044】

パスワードは、IKE認証に使用されるパスワードであり、認証ID同様、IPSecを使用可能な物理ポート毎に割り当てられる。フィールド207には、パスワード設定方式としてPre-Shared方式を使用している場合にはパスワード文字列が、デジタル署名を使用している場合には認証局から発行されたデジタル署名がパスワードとして格納される。例えば、図2に示す例において、Host1が持つIPアドレス10.10.10.101の物理ポート115については、認証IDとしてIPアドレス、パスワード設定方法としてPre-Shared方式を用いることで、フィールド206へは10.10.10.101、フィールド207へはパスワード文字列aaaaaaという値が格納されている。

【0045】

ポート情報テーブル134は管理サーバ103により管理される。管理サーバ103は、システムに新しい物理ポート115等が追加されたり、新たに物理ポート115等へボリュームが割り当てられたり、パスワードの設定が行われる度にポート情報テーブル134を更新する。

【0046】

図3は、ストレージ容量管理テーブル135の構成例を示す図である。ストレージ容量管理テーブル135は、IPネットワーク104へ接続している記憶装置システム102が有する記憶領域の使用状況の情報を保持するテーブルである。

ストレージ容量管理テーブル135は、IPネットワーク104に接続されている記憶装置システム102の数分のエントリを有する。各エントリは、対応する記憶装置システム102の識別子である装置IDを登録するフィールド301、対応する記憶装置システム102の空き容量の情報を登録するフィールド302及び対応する記憶装置システム102の使用容量の情報を登録するフィールド303を有する。

【0047】

空き容量は、記憶装置システム 102 において、ディスクドライブ群 121 が有する記憶領域のうち、物理ボリュームが作成されていない記憶領域の記憶容量を示す情報である。また、使用容量はディスクドライブ群 121 が有する記憶領域のうち、すでに物理ボリュームとして使用されている記憶領域の記憶容量を示している。

例えば図 3 に示す例では、Storage 1 が有する記憶領域のうち、空き容量は 10 T バイトであり、使用容量は 5 T バイトである。ストレージ容量管理テーブル 135 はネットワーク管理プログラム 132 により管理される。ネットワーク管理プログラム 132 は、IP ネットワーク 104 へ接続している記憶装置システムへ新しい物理ボリュームが作成される度（あるいは削除される度）にストレージ容量管理テーブル 135 の内容を更新する。

【0048】

図 4 は、サーバ 101 が保持するパス情報テーブル 111 の構成例を示す図である。パス情報テーブル 111 は、サーバ 101 が IP ネットワーク 104 を介して使用する仮想的な記憶装置（以下「ディスクデバイス」）の名前と、サーバ 101 がディスクデバイスへアクセスするための情報を保持するテーブルである。パス情報テーブル 111 は、サーバ 101 が使用するディスクデバイスの数分のエントリを有する。

【0049】

個々のエントリは、対応するディスクデバイスに対してサーバ 101 で付与された名前であるデバイス名を登録するフィールド 401、対応するディスクデバイスを含む SCSI オブジェクトのオブジェクト ID を登録するフィールド 402、ディスクデバイスに対応するボリュームの LUN を登録するフィールド 403、対応するディスクデバイスを含む SCSI オブジェクトに割り振られた物理ポートの IP アドレスを登録するフィールド 404 及び対応するディスクデバイスを含む SCSI オブジェクトに割り振られた物理ポートの TCP ポート番号が登録されるフィールド 405 を有する。

【0050】

ここで、ディスクデバイスとは、サーバ 101 で実行されるオペレーティングシステム（「OS」）等のプログラムにおいて扱われる記憶領域の単位である。ディスクデバイスは一つ又は複数のボリュームから構成される。本実施形態では、デバイス名の例として、例えば、図 4 に示すように「/dev/had」等の名前が用いられる。パス情報テーブル 111 の内容は、システムの管理者が手動で設定しても良いし、ホスト 101 上の OS やパス管理プログラム 110 が任意にデバイス名等を設定しても良い。

【0051】

尚、1 つの SCSI オブジェクト（例えば SCSI ターゲット）が複数のディスクデバイスを有していても良く、逆に複数の SCSI オブジェクトから一つのディスクデバイスが構成されていても良い。又、SCSI オブジェクトは、1 つ又は複数のボリュームから構成される。

【0052】

図 5 は、記憶装置システム 102 が保持するボリューム情報テーブル 123 の構成例を示す図である。ボリューム情報テーブル 123 は、各記憶装置システム 102 で作成された物理ボリュームの特性に関する情報を保持するテーブルである。ボリューム情報テーブル 123 は、記憶装置システム 102 が有する物理ボリュームの数分のエントリを有する。各エントリは、対応する物理ボリュームの識別子である物理ボリューム番号を登録するフィールド 501、物理ボリュームに対応するボリュームの LUN を登録するフィールド 502、対応する物理ボリュームの容量を登録するフィールド 503、対応する物理ボリュームを含む SCSI オブジェクトのオブジェクト ID を登録するフィールド 506、対応する物理ボリュームを含む SCSI オブジェクトに対応付けられた物理ポートに割り振られた IP アドレスを登録するフィールド 504、対応する物理ボリュームを含む SCSI オブジェクトと TCP コネクションを確立するために使用する TCP ポートのポート番号を登録するフィールド 505 及び物理ボリュームに対応する物理ポートを有する HBA 等が IPsec 処理部を持つか否かを示す情報を登録するフィールド 507 を有する。

【0053】

ボリューム情報テーブル 123 は、記憶装置システム 102 により管理される。記憶装

置システム102は、物理ボリュームを作成し、その物理ボリュームからボリュームを作成することによって作成したボリュームの特性をボリューム情報テーブル123へ登録する。

【0054】

図6は、IPネットワーク104へ接続している装置が保持するパスワード管理テーブル124の構成例を示す図である。パスワード管理テーブル124は、そのテーブルを保持している装置が暗号化通信を行う相手の数分のエントリを有する。パスワード管理テーブルの各エントリは、IPSecを用いた暗号化通信を行う通信相手に対する認証IDの情報を登録するフィールド601及び暗号化通信の際にIKEでの認証に用いるパスワードを登録するフィールド602とを有する。

パスワード管理テーブル112は、パスワードの登録が行われる度に更新される。

【0055】

本実施形態では、サーバ101の使用者（あるいは管理者）が記憶装置システム102の記憶領域を新たに使用したい場合、使用者は管理サーバ103に対してボリュームの作成要求を発行する。この際、使用者は、作成したいボリュームの特性（ここではセキュリティレベル）についての要求もボリューム作成の要求に含める。ボリュームの作成要求を受領した管理サーバ103は、使用者の要求（ここでは記憶容量とセキュリティレベル）に応じたボリュームが作成可能な記憶装置システム102をポート情報テーブル134及びストレージ容量管理テーブル135から検索する。

【0056】

検索の結果、使用者の要求に合致する記憶装置システム102が検索された場合、管理サーバ103は、検索された記憶装置システム102に対して、使用者が要求するボリュームの作成を指示する。特に、高いセキュリティレベル（ここではIPSecによる暗号化通信）が使用者から要求される場合には、管理サーバ103は、記憶装置システム102に対して、作成したボリュームをIPSec処理部を有するHBA等が有する物理ポート（以下「IPSec機能を有する物理ポート」とも言う）に割り付けるように指示する。

【0057】

その後、記憶装置システム102からボリューム作成の完了を受信した管理サーバ103は、ボリューム作成の完了とそのボリュームを使用するための情報（ボリュームと対応付けられたIPアドレス等）を使用者（サーバ101や管理者）に送信する。ボリューム作成完了の通知を受けた使用者は、受信した情報を用いて、作成されたボリュームを使用（ボリュームを用いたディスクデバイスの作成等）する。サーバ101がセキュリティが確保されたボリュームに対して通信を行う際は、サーバ101は、IPSecのプロトコルにのっとり、まず認証ID及びパスワードを、ボリュームを有する記憶装置システム102に送信する。記憶装置システム102は、送信された認証ID及びパスワードを用いて、サーバ101の認証を行う。サーバ101が記憶装置システム102に認証された後、サーバ101は、ボリュームに格納するデータを暗号化して記憶装置システム102へ送信する。

【0058】

以下、本実施形態の処理手順の詳細について説明する。

図7は、本実施形態におけるボリューム割り当て処理全体の手順を示す図である。まず、管理サーバ103は、サーバ101や管理者からのボリューム作成要求を受信するまで構成情報管理処理を行っている（ステップ701）。管理サーバ103は、サーバ101や管理者からボリューム作成要求を受信する（ステップ702）と、ボリューム作成と割り当て処理703を実行する。この処理により、サーバ101が新しいボリュームを使用することが出来る。ステップ701及び703での処理の詳細は後述する。

【0059】

図8は、管理サーバ103が実行する構成情報管理処理の手順を示す図である。構成情報管理処理では、管理サーバ103が、IPネットワーク104への新しい物理ポート115等の追加、追加された物理ポートのIPSec機能の有無、記憶装置システム102の容量追加等を検知し、各種テーブルの内容を更新する。

【0 0 6 0】

管理サーバ 1 0 3 は、サーバ 1 0 1 等からボリューム作成の指示を受けつけていない場合は、常に（又は一定の間隔、任意の時間に）IPネットワーク 1 0 4 に新しい物理ポート 1 1 5 等が接続されたかどうかを探索している。具体的には、システムの管理者が手動で物理ポートの追加を管理サーバ 1 0 3 に通知しても良いし、管理サーバ 1 0 3 が管理用ネットワーク 1 0 5 を通じてIPネットワーク 1 0 4 に接続される装置の構成情報を定期的に収集しても良い。

【0 0 6 1】

IPネットワーク 1 0 4 に接続される装置の構成情報を定期的に収集する方法の一例としては、管理サーバ 1 0 3 がSNMP(Simple Network Management Protocol)を用いてIPネットワーク 1 0 4 に接続される装置からMIB(Management Information Base)を収集する方法がある。また、そのほかに、管理用ネットワーク 1 0 5 にiSNS (Internet Storage Name Service) サーバが接続している場合は、管理サーバ 1 0 3 が、iSNSサーバが発行するSCN(State Change Notification)を管理用ネットワーク 1 0 5 経由で検知する方法もある。ここで、iSNSとは、Internet draftである「Internet Storage Name Service」にて規定される公知技術であり、IP-SANデバイス及びFC-SANデバイスを発見、識別、管理する機能を提供できる（参考 <URL : <http://www.ietf.org/internet-drafts/draft-ietf-ips-isns-21.txt>>）（ステップ 8 0 1）。

【0 0 6 2】

ネットワーク 1 0 4 に新たな物理ポートが追加されたことを検出した場合、管理サーバ 1 0 3 は、新しく追加された物理ポートのIPSec機能の有無、物理ポートをもつ装置の装置ID及びその装置のノード種別を収集する。そして、管理サーバ 1 0 3 は、収集した情報をポート情報テーブル 1 3 4 へ登録する。情報の収集方法は、例えばシステムの管理者が手動で管理サーバ 1 0 3 へ入力する方法でも良いし、管理サーバ 1 0 3 がMIB等を用いて追加された物理ポートを有する装置から自動的に収集しても良い（ステップ 8 0 2）。

【0 0 6 3】

その後、管理サーバ 1 0 3 は、新しく追加された物理ポートへIPアドレスとオブジェクトIDを割り当てる。ただし、オブジェクトIDに関しては、このステップで割り当てなくとも良い。この場合、オブジェクトIDは管理サーバ 1 0 3 及び記憶装置システム 1 0 2 が実行するボリューム作成と割り当て処理の際に物理ポートに割り当てられる。IPアドレスの割り当て方法は、システムの管理者が手動で管理サーバ 1 0 3 へIPアドレスを入力しても良いし、管理サーバ 1 0 3 がDHCP (Dynamic Host Configuration Protocol) 等のプログラムを利用してIPアドレスを自動的に割り当てても良い。

【0 0 6 4】

オブジェクトIDの割り当て方法は、システムの管理者が手動で管理サーバ 1 0 3 へオブジェクトIDを入力しても良いし、新しく追加された物理ポートを持つ装置がポートに自動的にオブジェクトIDを割り当てても良い。管理サーバ 1 0 3 は、割り当てられたIPアドレスとオブジェクトIDをシステムの管理者による通知やMIB等の情報により検知し、ポート情報テーブル 1 3 4 へ登録する。オブジェクトIDの割り当てを行わなかった場合には、図 2 において、装置IDがStorage2である記憶装置システム 1 0 2 の、割り当てIPアドレスが10.10.10.204である物理ポートのように、フィールド 2 0 2 が空欄となる（ステップ 8 0 3）。

【0 0 6 5】

その後、管理サーバ 1 0 3 は、ステップ 8 0 2 で収集した情報に基づいて、追加された物理ポートがIPSecの機能を有するかどうか（具体的には、追加された物理ポートを有するHBA等がIPSec処理部を有するかどうか）を判定する（ステップ 8 0 4）。

追加された物理ポートがIPSec機能を有する場合、管理サーバ 1 0 3 は、追加された新しい物理ポートがIKE認証で用いる認証IDとパスワードの設定を行う。管理サーバ 1 0 3 は、システムの管理者へ認証IDとパスワードを設定するよう通知する。管理者等は、管理サーバ 1 0 3 が有する入力インターフェースを介して新しい物理ポートについての

認証IDとパスワードの情報を入力する。管理サーバ103は、入力された認証IDとパスワードを、ポート情報テーブル134に登録する（ステップ805）。

【0066】

ステップ801で新しい物理ポートを発見しなかった場合、ステップ804で新しく追加された物理ポートがIPSec機能を有さなかった場合又はステップ805の処理の後、管理サーバ103は、IPネットワークに接続される記憶装置システム102の記憶容量の変化や新しく接続された物理ポートを有する装置が記憶装置システム102であるかどうかを判定する。管理サーバ103が新しい記憶装置システム102の追加を検出する方法や既存の記憶装置システム102の記憶容量の記憶容量の変化を検出する方法は、IPネットワーク104への物理ポートの接続の検出方法と同様である。すなわちシステムの管理者の手動設定やMIB等の構成情報の定期的な収集である（ステップ806）。

【0067】

記憶装置システム102の追加や既存の記憶装置システム102の記憶容量の変化を検出した管理サーバ103は、新しく追加された記憶装置システム102（又は変更があった記憶装置システム102）の記憶容量をストレージ容量管理テーブル135へ登録する。管理サーバ103が記憶装置システム102の記憶容量の情報を収集する方法も、上述の物理ポートの検出方法等と同じ方法が考えられる（ステップ807）。

【0068】

ステップ806で新しい記憶装置システム102の追加や記憶装置システム102の容量変化を検出しなかった場合又はステップ807の実行後、管理サーバ103は、ネットワーク104から物理ポートが削除（具体的にはネットワーク104から物理ポートが外されること）されたかを判定する。管理サーバ103が物理ポートの削除を検出する方法は、削除されたポートのIPアドレスを、システムの管理者による通知や定期的に収集したMIB等の情報より検知する方法が考えられる（ステップ808）。

【0069】

ネットワーク104から削除された物理ポートのIPアドレスを検知した管理サーバ103は、ポート情報テーブル134のフィールド303を検索することで削除された物理ポートの情報を特定し、同情報をポート情報テーブル134から削除する（ステップ809）。

【0070】

図9及び図10は、管理サーバ103及び記憶装置システム102が実行するボリューム作成と割り当て処理の手順を示す図である。ボリューム作成と割り当て処理は、サーバ101や管理者からボリュームの作成要求を受けた際に実行される。サーバ101や管理者から管理サーバ103へ送信されるボリューム作成要求には、作成されるボリュームに必要な記憶容量、作成されるボリュームへのアクセスのセキュリティレベル、例えばボリュームへアクセスする際にIPSecによる暗号化が必要か否かの情報が含まれる。

【0071】

最初に管理サーバ103は、ボリューム作成要求に含まれるボリュームへのアクセスについてのセキュリティレベルの情報に基づいて、作成が要求されたボリュームへのアクセスについてIPSecによる暗号化通信が必要か否かの判定を行う（ステップ901）。

作成が要求されるボリュームへのアクセスについてIPSecに基づく暗号化通信が不要であると判断した場合、管理サーバ103は、ポート情報テーブル134のフィールド305を検索し、IPSec機能を持たない物理ポートを特定する。そして、管理サーバ103は、特定した物理ポートのIPアドレス及び物理ポートを保持する記憶装置システム102の装置IDを特定する。次に管理サーバ103は、特定した装置IDでストレージ容量管理テーブル135を検索し、特定した装置IDを有する記憶装置システム102の空き容量を確認する。そして管理サーバ103は、特定した装置IDを有する記憶装置システム102の中から、作成が要求されたボリュームの記憶容量以上の空き容量を有する記憶装置システム102を特定する（ステップ902）。

【0072】

次に管理サーバ103は、ステップ902で特定した記憶装置システム102へ、サーバや管理者から要求された記憶容量を有するボリュームの作成を指示する命令を発行する。

ボリューム作成の命令を受信した記憶装置システム102は、要求された記憶容量のボリュームを作成する。ボリューム作成を終了した記憶装置システム102は、ボリューム作成の終了を管理サーバ103へ送信する。

【0073】

ボリューム作成終了の通知を受信した管理サーバ103は、ボリュームを作成した記憶装置システム102に対して、作成したボリュームをIPSec機能を持たない物理ポートへ割り当てることを指示する命令を発行する。この命令には、管理サーバ103がステップ902で収集した、特定された記憶装置システム102が有するIPSec機能を持たない物理ポートに割り振られたIPアドレスの情報が含まれる。

【0074】

管理サーバ103からポート割り当て命令を受けた記憶装置システム102は、作成したボリュームを指定された物理ポートへ割り当てる。

【0075】

続いて記憶装置システム102は、作成したボリュームへTCPコネクションを確立する際に使用するTCPポート番号を決定する。TCPポート番号を決定する方法は、記憶装置システム102が自動的に決定しても良いし、ボリューム作成要求を発行したサーバ101や管理者へTCPポート番号を決めるように促しても良い。また、管理サーバ103がポート割り当て命令を発行する前に、管理サーバ103が自動的にTCPポート番号を決定する、或いは、管理サーバ103がボリューム作成要求を発行したサーバ101や管理者へTCPポート番号を決定するよう促し、決定したTCPポート番号をポート割り当て命令に含める方法でも良い。割り当てを終了した記憶装置システム102は、その結果を管理サーバ103へ通知する（ステップ903）。

【0076】

上記の例では、管理サーバ103からボリューム作成命令とポート割り当て命令を別々に発行しているが、それらを一つにまとめた命令を発行する構成も考えられる。そのような構成におけるステップ903の動作手順を以下に説明する。

【0077】

管理サーバ103は、ステップ902で特定した記憶装置システム102へボリューム作成・ポート割り当て命令を発行する。この命令は、サーバや管理者から発行された記憶容量を有するボリュームの作成を指示する命令及び作成したボリュームをIPSec機能を有しない物理ポート125へ割り当てることを指示する命令を含む。また、この命令には、管理サーバ103がステップ902で収集した、特定された記憶装置システム102が有するIPSec機能を有しない物理ポートに割り振られたIPアドレスの情報が含まれる。さらに、作成したボリュームへTCPコネクションを確立する際に使用するTCPポート番号を含めても良い。

【0078】

ボリューム作成・ポート割り当て命令を受信した記憶装置システム102は、要求された記憶容量のボリュームを作成する。ボリューム作成に失敗した場合、記憶装置システム102は、管理サーバ103へエラー情報を発行する。ボリューム作成に成功した場合、記憶装置システム102は、作成したボリュームを指定された物理ポート125へ割り当てる。割り当てを完了した記憶装置システム102は、その結果を管理サーバ103へ通知する。

【0079】

ステップ902の処理で要求されたボリュームを作成可能な記憶装置システム102がシステム上に存在しなかったり、記憶装置システム102の故障などの理由によりステップ903で行われる処理が失敗した場合、管理サーバ103は、ボリューム作成要求を発行したサーバ101や管理者へエラー情報を通知し、ボリューム作成と割り当て処理を終

了する（ステップ 9 0 6）。

【0 0 8 0】

ステップ 9 0 2 及び 9 0 3 の処理が成功した場合、管理サーバ 1 0 3 は、ストレージ容量管理テーブル 1 3 5 及びボリューム情報テーブル 1 2 3 の内容の更新を行う。具体的には、管理サーバ 1 0 3 は、ストレージ容量管理テーブル 1 3 5 の内、ステップ 9 0 3 でボリュームを作成した記憶装置システム 1 0 2 の空き容量を作成したボリュームの容量分減らし、使用容量を作成したボリュームの容量分増加させる。

【0 0 8 1】

また管理サーバ 1 0 3 は、ステップ 9 0 3 でボリュームを作成した記憶装置システム 1 0 2 に対し、ボリューム情報テーブル 1 2 3 の更新を指示する命令を発行する。更新指示の命令を受けた記憶装置システム 1 0 2 は、ステップ 9 0 3 で作成したボリュームに対応する物理ボリュームの物理ボリューム番号、ボリュームへ割り当てた L U N、ボリュームの記憶容量、ボリュームを割り当てたポートの IP アドレス、ボリュームへ T C P コネクションを確立する際に使用する T C P ポート番号、ボリュームに割り当てられたオブジェクト I D 及びボリュームを割り当てたポートの IP S e c 機能の有無を含むエントリをボリューム情報テーブル 1 2 3 へ追加する。

【0 0 8 2】

ただし、図 2 において、装置 I D が Storage 2 である記憶装置システム 1 0 2 の、割り当て IP アドレスが 10. 10. 10. 204 である物理ポート 1 2 5 のように、オブジェクト I D が割り当てられていない物理ポート 1 2 5 も存在する。そのような物理ポート 1 2 5 をボリュームへ割り当ててる場合、オブジェクト I D の割り当てが行われる。オブジェクト I D の割り当て方法として、管理サーバ 1 0 3 がシステム管理者へオブジェクト I D を入力するよう促し、システムの管理者が手動で管理サーバ 1 0 3 へオブジェクト I D を入力し、管理サーバ 1 0 3 が、そのオブジェクト I D を、ボリューム情報テーブル 1 2 3 の更新指示を記憶装置システム 1 0 2 へ通知する方法がある。また、ボリュームを割り当てられた物理ポートを持つ装置がその物理ポートへ自動的にオブジェクト I D を割り当ててる方法でも良い（ステップ 9 0 5）。

【0 0 8 3】

ステップ 9 0 5 の終了後、管理サーバ 1 0 3 は、ボリューム作成要求を発行したサーバ 1 0 1 や管理者へ対し、ボリューム作成完了通知を発行する。ボリューム作成完了通知には、作成したボリュームへのアクセス経路に関する情報、つまり、作成したボリュームを割り当てた物理ポートの IP アドレス、TCP ポート番号、ボリュームへ割り当てた L U N、ボリュームに割り当てられたオブジェクト I D が含まれる（ステップ 9 0 7）。

【0 0 8 4】

一方、ステップ 9 0 1 で IP S e c による暗号化通信を必要とするボリュームであると判断された場合、管理サーバ 1 0 3 は、ポート情報テーブル 1 3 4 のフィールド 2 0 5 を検索し、IP S e c 機能を有する物理ポートを特定する。そして、管理サーバ 1 0 3 は、特定した物理ポートの IP アドレス及び物理ポートを保持する記憶装置システム 1 0 2 の装置 I D を特定する。次に管理サーバ 1 0 3 は、特定した装置 I D でストレージ容量管理テーブル 1 3 5 を検索し、特定した装置 I D を有する記憶装置システム 1 0 2 の空き容量を確認する。そして管理サーバ 1 0 3 は、特定した装置 I D を有する記憶装置システム 1 0 2 の中から、作成が要求されたボリュームの記憶容量以上の空き容量を有する記憶装置システム 1 0 2 を特定する（図 1 0 のステップ 1 0 0 1、1 0 0 2）。

【0 0 8 5】

次に管理サーバ 1 0 3 は、ステップ 1 0 0 2 で特定した記憶装置システム 1 0 2 へ、サーバや管理者から要求された記憶容量を有するボリュームの作成を指示する命令を発行する。

ボリューム作成の命令を受信した記憶装置システム 1 0 2 は、要求された記憶容量のボリュームを作成する。ボリューム作成を終了した記憶装置システム 1 0 2 は、ボリューム作成の終了を管理サーバ 1 0 3 へ送信する。

【0086】

ボリューム作成終了の通知を受信した管理サーバ103は、ボリュームを作成した記憶装置システム102に対して、作成したボリュームをIPSec機能を有する物理ポートへ割り当てることを指示する命令を発行する。この命令には、管理サーバ103がステップ1002で収集した、特定された記憶装置システム102が有するIPSec機能を有する物理ポートに割り振られたIPアドレスの情報が含まれる。

【0087】

管理サーバ103からポート割り当て命令を受けた記憶装置システム102は、作成したボリュームを指定された物理ポートへ割り当てる。割り当てを完了した記憶装置システム102は、その結果を管理サーバ103へ通知する（ステップ1003）。

【0088】

上記の例では、管理サーバ103からボリューム作成命令とポート割り当て命令を別々に発行しているが、それらを一つにまとめた命令を発行する構成も考えられる。そのような構成におけるステップ1003の動作手順を以下に説明する。

【0089】

管理サーバ103は、ステップ1002で特定した記憶装置システム102へボリューム作成・ポート割り当て命令を発行する。この命令は、サーバや管理者から発行された記憶容量を有するボリュームの作成を指示する命令及び作成したボリュームをIPSec機能を有する物理ポートへ割り当てることを指示する命令を含む。また、この命令には、管理サーバ103がステップ1002で収集した、特定された記憶装置システム102が有するIPSec機能を有する物理ポートに割り振られたIPアドレスの情報が含まれる。

【0090】

ボリューム作成・ポート割り当て命令を受信した記憶装置システム102は、要求された記憶容量のボリュームを作成する。ボリューム作成に失敗した場合、記憶装置システム102は、管理サーバ103へエラー情報を発行する。

【0091】

ボリューム作成に成功した場合、記憶装置システム102は、作成したボリュームを物理ポートへ割り当てる。割り当てを完了した記憶装置システム102は、その結果を管理サーバ103へ通知する。

【0092】

ステップ1002の処理で要求されたボリュームを作成可能な記憶装置システム102がシステム上に存在しない場合、IPSec機能を有する物理ポートが無い場合又は記憶装置システム102の故障などの理由によりステップ1003で行われる処理が失敗した場合、管理サーバ103は、ボリューム作成要求を発行したサーバ101や管理者へエラー情報を通知し、ボリューム作成と割り当て処理を終了する（ステップ1008）。

【0093】

ステップ1002及び1003の処理が成功した場合、管理サーバ103はIPSecアカウント処理を行う。IPSecアカウント処理とは、IKE認証に使用するパスワードを、IPSecを使用する装置に登録する処理である。IPSecアカウント処理の詳細は図11にて説明する。

【0094】

IPSecアカウント処理の後、管理サーバ103は、ストレージ容量管理テーブル135及びボリューム情報テーブル123の内容の更新を行う。具体的には、管理サーバ103は、ストレージ容量管理テーブル135の内、ステップ1003でボリュームを作成した記憶装置システム102の空き容量を作成したボリュームの容量分減らし、使用容量を作成したボリュームの容量分増加させる。

【0095】

また管理サーバ103は、ステップ1003でボリュームを作成した記憶装置システム102に対し、ボリューム情報テーブル123の更新を指示する命令を発行する。更新指示の命令を受けた記憶装置システム102は、ステップ1003で作成したボリュームに

対応する物理ボリュームの物理ボリューム番号、ボリュームへ割り当てたLUN、ボリュームの記憶容量、ボリュームに割り当てられたオブジェクトID、ボリュームに割り当てられたオブジェクトID及びボリュームを割り当てたポートのIPSec機能の有無を含むエントリをボリューム情報テーブル123へ追加する（ステップ1006）

ステップ1006又はステップ1008の実行後、管理サーバ103は、ボリューム作成要求を発行したサーバ101や管理者へ対し、ボリューム作成完了通知が発行される。以上で、要求されたボリュームのボリューム作成と割り当て処理は完了する。

【0096】

尚、ボリューム作成完了通知を受けたサーバ101は、作成したボリュームをディスクデバイスとして取り扱うため、該ボリュームへデバイス名を付与する。デバイス名を付与する方法は、サーバ101上で動作するOSが自動的に決めても良いし、サーバ101のユーザが手動で決定しても良い。その後、サーバ101は、ボリュームへ付与したデバイス名と、ボリューム作成完了通知に含まれたボリュームへアクセスするための経路情報、すなわち、ボリュームに割り当てられたオブジェクトID、ボリュームへ割り当てたLUN、ボリュームを割り当てたポートのIPアドレス及びTCPポート番号をパス情報テーブル111へ追加する。

【0097】

尚、サーバ101等からのボリューム作成要求にはセキュリティレベル（暗号化の要否）の情報を含まない構成も考えられる。この場合、サーバ101が潜在的に要求するセキュリティレベルを判断するため、管理サーバ103は、ボリューム作成要求を発行したサーバ101がIPSec機能を有する物理ポート115aを有するかどうか判断する。具体的には、管理サーバ103が、ボリューム作成要求を発行したサーバ101のIPアドレスを元にポート情報テーブル134を検索してサーバ101がIPSec機能を持つ物理ポート115aを保持するかを特定する。

【0098】

ボリューム作成要求を発行したサーバ101がIPSec機能を持つ物理ポート115aを保持している場合、管理サーバ103は、作成が要求されるボリュームへのアクセスに対してセキュリティをかける必要があると判断する。そして、管理サーバ103は、作成したボリュームへIPSec機能を持つ物理ポートを割り当てよう、記憶装置システム102に指示する。一方、ボリューム作成要求を発行したサーバ101がIPSec機能を持つ物理ポート115aを保持していない場合、管理サーバ103は、作成が要求されるボリュームへのアクセスに対してセキュリティをかける必要が無いと判断する。そして、管理サーバ103は、作成したボリュームへIPSec機能を持たない物理ポート115bを割り当てよう、記憶装置システム102へ指示する。

【0099】

図11は、管理サーバ103が実行するIPSecアカウント処理の詳細な手順例を示す図である。

ボリューム割り当て処理のステップ702において、サーバ101がボリューム作成要求を発行した場合、IPSecアカウント処理を開始した管理サーバ103は、ボリューム作成要求を発行したサーバ101が持つ物理ポート115及びステップ903もしくはステップ1003でボリュームを割り当てられた物理ポート125が持つ認証ID及びパスワードを、ポート情報テーブル134を検索することにより特定する。ここでは、管理サーバ103は、物理ポートに割り当てられたIPアドレスに基づいて、各々の物理ポートの認証ID及びパスワードをポート情報テーブル134から検索する。

【0100】

また、ボリューム割り当て処理のステップ702において、管理者がボリューム作成要求を発行した場合、IPSecアカウント処理を開始した管理サーバ103は、管理者へ、作成したボリュームへのアクセスを許可するサーバ101を指定するよう要求を発行する。管理者からのアクセス許可サーバ情報（アクセスを許可するサーバ101の装置ID）を受けた管理サーバ103は、それらのサーバ101が持つ物理ポート115及びステップ

903もしくはステップ1003でボリュームを割り当てられた物理ポートが持つ認証ID及びパスワードを、ポート情報テーブル134を検索することにより特定する。

【0101】

ここでは、管理サーバ103は、アクセスを許可すべきサーバ101（以下「アクセス許可サーバ101」）が持つ物理ポート115aの認証ID及びパスワードをアクセス許可サーバ101の装置IDに基づいて、また、ボリュームを割り当てられた物理ポート125が持つ認証ID及びパスワードを物理ポート125aに割り当てられたIPアドレスに基づいてポート情報テーブル122から検索する（ステップ1101）。

【0102】

各々の物理ポートの認証ID及びパスワードを特定した管理サーバ103は、ステップ1101で特定した認証IDとパスワードの内、サーバ101が有する物理ポート115を用いる際に使用される認証ID及びパスワードを記憶装置システム102が保持するパスワード管理テーブルへ登録する指示を記憶装置システム102へ送信する。又管理サーバ103は、特定した認証IDとパスワードの内、記憶装置システム102が有する物理ポート125aを用いる際に使用される認証IDとパスワードをサーバ101が保持するパスワード管理テーブルへ登録する指示をサーバ101へ送信する。

【0103】

尚、上述の例では、サーバ101等が高いセキュリティレベルを要求しない場合、作成したボリュームをIPSec機能を有さない物理ポートに割り当てるように管理サーバ103は管理していた。しかし、必ずしもこのようにする必要は無く、サーバ101等から高いセキュリティレベルの要求が無くても、管理サーバ103が、作成したボリュームをIPSec機能を有する物理ポートに割り当てよう管理しても良い。この様にするとユーザが要求する以上のセキュリティが確保されてしまうが、空き領域を有する記憶装置システムがIPSec機能を有する物理ボリュームしかない場合でもボリュームの割当てをすることができる。

【0104】

上述した第一の実施形態においては、管理サーバ103からサーバ101へボリュームの作成報告をする際に、ボリュームが作成された記憶装置システム102への経路情報と一緒に送付されていた。しかしこれでは、他のサーバ101は作成されたボリュームへのアクセスに必要な情報を得られない。したがって、作成されたボリュームはボリューム作成が通知されたサーバ101でしか使用できない。

【0105】

一方iSCSIでは、サーバが任意の記憶装置システム102が有するオブジェクト（ターゲット）を見つける（経路情報を取得する）処理（ディスカバリ）が規定されている。これにより、iSCSIでは、複数のサーバ101がボリュームへのアクセスに関する経路情報を共有することが出来る。そこで、第二の実施形態として、第一の実施形態における管理サーバ103で、ディスカバリの処理をポート割当ての処理と連携して行う実施形態を考える。

【0106】

尚、ディスカバリとは、SCSIイニシエータがSCSIターゲットにログインするために必要な情報を、SCSIターゲットに割り振られたネームを管理する計算機（以下「ネーム管理サーバ」）に問い合わせ得る事を指す。iSCSIに対応するネーム管理プロトコルの例としては、iSNSや、Internet draftである「Finding iSCSI Targets and Name Servers Using SLP」にて規定されるSLP(Service Location Protocol)がある（参考 <URL: <http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-slp-06.txt>>）。

【0107】

図12は、第二の実施形態におけるシステム構成例を示した図である。以下、第一の実施形態と異なる点のみ説明する。第二の実施形態における第一の実施形態との主な相違点は、管理サーバ103が、第一の実施形態の管理サーバ103の構成に加え、ネーム管理サーバの構成を有する点である。尚、以下の説明においては第一の実施形態と同じものに

ついては同じ番号を振るものとする。

【0108】

管理サーバ103は、第一の実施形態と同様に一般的な計算機であり、プロセッサ、メモリ、及びネットワーク接続部を有する。メモリには、ネットワーク管理プログラム132、ネーム管理プログラム1201及び構成データベース133が格納される。

構成データベース133は、ポート情報テーブル134、ストレージ容量管理テーブル135及びアクセス経路情報テーブル1202を有する。

【0109】

管理サーバ103は、ネットワーク管理プログラム132を実行することで、第一の実施形態での処理に加え、ボリューム作成の終了後、作成したボリュームへのアクセス経路（具体的には、アクセスするための必要な情報）及びボリュームへアクセス可能なサーバ101のオブジェクトIDを、自身が有するアクセス経路情報テーブル1202へ登録する処理を行う。これにより、管理サーバ103が複数のサーバ101に対して同じボリュームへのアクセス経路の情報を提供することが出来る。

【0110】

又、管理サーバ103は、ネーム管理プログラム1201を実行することで、IPネットワーク104へ接続するサーバ101から受信したSCSIターゲットのディスクバリ要求に対して、アクセス経路情報テーブル1202を参照して前記SCSIターゲットへのログインに必要な情報を特定する。そして、管理サーバ103は、特定した情報をディスクバリ要求を送信したサーバ101へ送信する。

【0111】

ここでネーム管理プログラム1201としてiSNSを用いた場合、管理サーバ103は、ディスクバリ要求で要求されるSCSIターゲットのオブジェクトID、IPアドレス、TCPポート番号をサーバ101へ通知する。なお、図12に示した構成例ではネーム管理プログラム1201及びアクセス経路情報テーブル1202を管理サーバ103のメモリ129内に格納しているが、それらを管理サーバ103とは別の計算機で動作させる構成にしても良い。

【0112】

図13は、アクセス経路情報テーブル1202の構成例を示す図である。アクセス経路情報テーブル1202は、ネットワーク104に接続されたサーバ101が、ネットワーク104に接続された記憶装置システム102が保持するSCSIターゲットへアクセスするために必要な経路情報を管理するテーブルである。アクセス経路情報テーブル1202は、ネットワーク104に接続される記憶装置システム102が有するSCSIターゲットの数分のエントリを有する。

【0113】

各エントリは、エントリに対応するSCSIターゲットに割り振られたオブジェクトIDを登録するフィールド1301、SCSIターゲットに割り振られたIPアドレスを登録するフィールド1302、SCSIターゲットのIPアドレスに対応するTCPポート番号を登録するフィールド1303及び対応するSCSIターゲットにアクセス可能なサーバ101に割り振られているオブジェクトIDを格納するフィールド1304を有する。

【0114】

一つのエントリのフィールド1304には、エントリに対応するSCSIターゲットへアクセス可能なサーバ101の数分のオブジェクトIDが格納される。管理サーバ103は、ボリューム作成が行われる度、アクセス経路情報テーブル1202を更新する。

【0115】

尚、アクセス経路情報テーブル1202に保持される情報は、ネーム管理に使用されるプロトコルに依存する。ネーム管理プログラム1201がその他の属性を管理する場合、アクセス経路情報テーブル1202は該属性に関する情報も格納される。

【0116】

図14は、本実施形態におけるボリューム割り当て処理全体の流れを示す図である。本

実施形態におけるボリューム割り当て処理のうち、ステップ1401及び1402の処理は第一の実施形態における図8のステップ701及び702と同じであるので、説明を省略する。ステップ1402でサーバ101または管理者等からボリューム作成の指示を検出した管理サーバ103は、ボリューム作成と割り当て処理1403及びアクセス経路通知処理1404を実行する。ボリューム作成と割り当て処理1403及びアクセス経路通知処理1404の詳細は後述する。

【0117】

図15及び図16は、管理サーバ103及び記憶装置システム102で実行されるボリューム作成と割り当て処理（図14のステップ1403）の流れを示す図である。尚、第一の実施形態と同様に、サーバ101や管理者から管理サーバ103に送信されるボリューム作成要求には、ボリュームに必要な記憶容量と要求するセキュリティレベル（ここでは作成するボリュームへアクセスする際にIPSecによる暗号化が必要か否か）の情報が含まれる。尚、第一の実施形態と同様に、セキュリティレベルを管理サーバ103がサーバ101の物理ポートの特性に応じて決定しても良い。

【0118】

図15において、ステップ1501～1505及びステップ1508で行われる処理は第一の実施形態におけるボリューム作成と割り当て処理（図9）のステップ901～906で行われる処理と同一であるので、説明を省略する。又、図16において、ステップ1601～1606及び1609で行われる処理は、第一の実施形態におけるボリューム作成と割り当て処理（図10）のステップ1001～1006及び1008で行われる処理と同一であるので、説明を省略する。

【0119】

図15においてステップ1505の処理の実行後、管理サーバ103は、ステップ1503で記憶装置システム102へ発行した物理ポートへの割り当て要求に含まれるIPアドレス、TCPポート番号、及びオブジェクトIDをアクセス経路情報テーブル1202へ新しいエントリとして登録する。更に、管理サーバ103は、ステップ1503で作成されたボリュームへアクセス可能なサーバ101を決定する。そして管理サーバ103は、決定されたサーバ101のオブジェクトIDを、アクセス経路情報テーブル1202に新しく追加されたエントリのフィールド1304へ登録する。

【0120】

尚、新たに作成されたボリュームへアクセス可能なサーバ101を決定する方法は種々存在する。例えば、ボリュームの作成要求を発行したのが管理者である場合には、管理サーバ103が管理者へ、作成したボリュームへアクセス可能なサーバ101を登録するように促す方法がある。又、ボリュームの作成要求を発行したのがサーバ101である場合には、管理サーバ103が、作成要求を発行したサーバ101を、作成されたボリュームにアクセス可能なサーバ101としてアクセス経路情報テーブル1202へ登録する方法でも良い。また、ネットワーク104に接続されるサーバ101を幾つかのグループに分割しておき、管理サーバ103が、ボリュームの作成要求を発行したサーバ101を含むグループ全てのサーバ101を、作成されたボリュームへアクセス可能なサーバ101としてアクセス経路情報テーブル1202へ登録する方法としても良い（ステップ1506）。

【0121】

その後、管理サーバ103は、ボリューム作成要求を発行したサーバ101や管理者へ対し、ボリューム作成完了通知（ここではアクセス経路に関する情報は含まれない）を発行する。以上で、要求されたボリュームが暗号化通信を必要としない場合のボリューム作成と割り当て処理は完了する。

【0122】

図16において、ステップ1606の実行後、管理サーバ103は、ステップ1603で記憶装置システム102へ発行した物理ポートへの割り当て要求に含まれるIPアドレス、TCPポート番号及びオブジェクトIDをアクセス経路情報テーブル1202の新しい

エントリとして登録する。

【0123】

更に管理サーバ103は、ステップ1603で作成されたボリュームへアクセス可能なサーバ101を決定する。そして管理サーバ103は、決定されたサーバ101のオブジェクトIDを、アクセス経路情報テーブル1202の新しく追加されたエントリのフィールド1304へ追加する。アクセス可能なサーバ101の決定方法は、図15の説明と同様である（ステップ1607）。

【0124】

その後、管理サーバ103は、ボリューム作成要求を発行したサーバ101や管理者へ対し、ボリューム作成完了通知（ここではアクセス経路情報は含まれない）を発行する。

【0125】

図17は、図14のステップ1405で行われるアクセス経路通知処理の手順例を示す図である。管理サーバ103は、アクセス経路情報テーブル1202を検索して、ステップ1403で作成したボリュームへ割り当てたオブジェクトID、IPアドレス、TCPポート番号、作成したボリュームへアクセス可能なサーバ101を特定する（ステップ1701）。

【0126】

次に管理サーバ103は、ステップ1701で特定したオブジェクトID、IPアドレス及びTCPポート番号を、ステップ1701で特定したサーバ101へ通知する。管理サーバ103がサーバ101へオブジェクトID等を通知する方法として、例えば、iSNSサーバの役割を果たす管理サーバ103がSCNをサーバ101へ発行し、ネットワーク104に接続されたサーバ101へディスカバリを要求する方法がある（ステップ1702）。

【0127】

尚、ネットワーク104に接続されたサーバ101は、管理サーバ103をネーム管理サーバ、本実施形態ではiSNSサーバとして扱う。したがって、サーバ101は、自身が使用するターゲットへのアクセス情報を得るため、管理サーバ103に対してディスカバリ要求を発行する。

【0128】

図18は、管理サーバ103がディスカバリ要求を受け取った際に行う処理（以下「ネーム問い合わせ処理」）の手順例を示した図である。

ディスカバリ要求に基づいた処理を受けつけていない場合、管理サーバ103はサーバ101からディスカバリ要求を受信したかどうかを監視している（ステップ1801）。

【0129】

サーバ101からディスカバリ要求を受信した管理サーバ103は、アクセス経路情報テーブル1202を検索し、ディスカバリ要求を発行したサーバ101がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ103は、ディスカバリ要求を発行したサーバ101がアクセス可能なSCSIターゲットのオブジェクトID、IPアドレス及びTCPポート番号をアクセス経路情報テーブル1202から取得する（ステップ1802）。

【0130】

その後管理サーバ103は、ステップ1802で取得したオブジェクトID、IPアドレス及びTCPポート番号を、ディスカバリ要求を発行したサーバ101へ通知する（ステップ1803）。

【0131】

本実施形態によれば、管理サーバ103が、記憶装置システム103が有するボリュームへのアクセス経路の情報を管理することにより、より柔軟に使用者等に対してボリュームを提供することができる。

【0132】

第2の実施形態の一つの変形例として、管理サーバ103等が、作成したボリュームに複数の物理ポートを割り当てることで、作成されたボリュームへのアクセス経路を複数提

供する構成がある。例えば、物理ポートとして、IPSecが使用できる物理ポートとIPSecが使用できない物理ポートの双方を、作成された1つのボリュームへ割り当てることができる。つまり、ボリュームへのアクセス経路を複数用意することができる。

【0133】

したがって、サーバ101が発行するディスクバリ要求に対し、管理サーバ103が、複数のアクセス経路の全てをサーバ101へ通知したり、複数のアクセス経路のうちの何れか、例えばディスクバリ要求を発行したサーバ101がIPSec機能を持つHBAを保持する場合には暗号化可能な物理ポートを使用するアクセス経路を、サーバ101がIPSec機能を持つHBAを保持していない場合には暗号化通信が行えない物理ポートを使用するアクセス経路を通知したりすることができる。又サーバ101が発行するディスクバリ要求に対し、IPSec機能を有する物理ポートを使用するアクセス経路全てあるいはIPSec機能を有さない物理ポートを使用するアクセス経路全てを通知しても良い。尚、サーバ101の物理ポートのIPSec機能の有無は、管理サーバ103がポート管理テーブルを参照することで確認できる。

【0134】

図19は、ボリュームに複数のポートを割り当てた場合のボリューム情報テーブル123の構成例を示す図である。ボリューム情報テーブル123は、基本的には図5で説明したボリューム情報テーブル123と同じ構成を有している。ただし、割り当てポートのIPアドレスを登録するフィールド1904と、割り当てポートのSCSIオブジェクトとTCPコネクションを確立する際に使用するTCPポート番号を登録するフィールド1905へそれぞれ複数のポートのIPアドレスとTCPポート番号を登録できる点が図5のボリューム情報テーブル123とは異なる。又、IPアドレスが複数登録できることに対応して、登録された各IPアドレスで示される物理ポートがIPSec機能を有するかどうかを示す情報を登録するフィールドが一つのオブジェクトに対して複数用意される点も図6とは異なる。例えば図19では、物理ボリュームVol. 0に対して、IPSec機能を持つ物理ポートのIPアドレス10.10.10.201と、IPSec機能を持たない物理ポートのIPアドレス10.10.10.202が割り当てられている。

【0135】

図20は、本変形例でのアクセス経路情報テーブル1202の構成例を示す図である。本変形例において、アクセス経路情報テーブル1202は、図14で説明したアクセス経路情報テーブル1202と異なり、一つのSCSIターゲットに対し複数のアクセス経路の情報を登録することができる。例えば、図20において、オブジェクトIDがiqn.2003-01.com.example:storage1であるSCSIターゲットに対し、IPSec機能を持つポートのIPアドレス10.10.10.201とTCPポート番号3260、IPSec機能を持たないポートのIPアドレス10.10.10.202とTCPポート番号3260の情報が登録されている。

【0136】

本変形例におけるボリューム割り当て処理では、ステップ1403で行われるボリューム作成と割り当て処理、及びステップ1404で行われるアクセス経路通知処理の手順が変更される。以下、変更点のみを記す。

【0137】

先ずボリューム作成と割り当て処理のステップ1501においては、判定が行われず、続いてステップ1601が実行される。ステップ1601、及びステップ1602にて行われる処理の内容に変更は無い。

【0138】

ステップ1603において、管理サーバ103は、作成したボリュームをIPSec機能を有する物理ポートと、IPSec機能を有しない物理ポートの両方へ割り当てよう、記憶装置システム102へ命令を発行する。なお、管理サーバ103が指定する、作成したボリュームを割り当てる物理ポート数は、2以上の任意の数である。

【0139】

ステップ1605にて行われるIPSecアカウント処理では、管理サーバ103は、ボリ

ュームへ割り当てたIPSec機能を有する物理ポートの認証ID及びパスワードを、作成したボリュームへのアクセスを許可するサーバ101が保持するパスワード管理テーブル112へ登録する。ボリュームへ割り当てられたIPSec機能を有する物理ポートが複数ある場合には、それら全ての物理ポートの認証ID及びパスワードがパスワード管理テーブル112へ登録される。

【0140】

ステップ1605にて行われるボリューム情報テーブル123の更新では、ステップ1603で記憶装置システム102がボリュームへ割り当てた全ての物理ポートのIPアドレス、TCPポート番号がボリューム情報テーブル123へ登録される。

【0141】

ステップ1608で行われるアクセス経路情報テーブル1202の更新では、ステップ1603で記憶装置システム102がボリュームへ割り当てた全ての物理ポートのIPアドレス、TCPポート番号、及び物理ポートがもつIPSec機能の有無がアクセス経路情報テーブル1202へ登録される。

【0142】

ステップ1405で行われるアクセス経路通知処理のステップ1702では、管理サーバ103は、ステップ1701で特定した作成したボリュームへアクセス可能なサーバ101に対し、ディスカバリを要求する。

【0143】

管理サーバ103は、サーバ101からディスカバリ要求を受信した際、アクセス経路情報テーブル1202を検索してディスカバリ要求を送信したサーバ101がアクセス可能なオブジェクトを特定する。その後管理サーバ103は、ポート情報テーブル134を検索して、ディスカバリ要求を送信したサーバ101が有する物理ポートの特性（ここではIPSec機能の有無）を確認する。そして、管理サーバ103は、ディスカバリ要求を送信したサーバ101がIPSec機能を持つHBAを保持していた場合には、特定したオブジェクトに割り振られている物理ポートのうち、IPSec機能を持つ物理ポートのIPアドレスとTCPポート番号をサーバ101に送信する。一方、サーバ101がIPSec機能を持つHBAを保持していなかった場合には、管理サーバ103は、特定したオブジェクトに割り振られている物理ポートのうち、IPSec機能を持たない物理ポートのIPアドレスとTCPポート番号をサーバ101に送信する。

【0144】

図21は、本変形例における管理サーバ103が行うネーム問い合わせ処理の流れを示す図である。ディスカバリ要求に基づいた処理を行っていない場合、管理サーバ103はサーバ101からディスカバリ要求を受信したかどうかを監視している（ステップ2101）。

【0145】

サーバ101からディスカバリ要求を受信した管理サーバ103は、ディスカバリ要求に含まれるサーバ101のIPアドレスの情報に基づいてポート情報テーブル134を検索し、ディスカバリ要求を送信したサーバ101の装置IDを特定する。その後、管理サーバ103は、特定した装置IDに基づいてポート情報テーブル134を検索し、ディスカバリ要求を送信したサーバ101がIPSec機能を持つHBAを保持しているかを特定する（ステップ2102、2103）。

【0146】

ディスカバリ要求を送信したサーバ101がIPSec機能を持つHBAを保持していた場合、管理サーバ103は、アクセス経路情報テーブル1202を検索し、ディスカバリ要求を発行したサーバ101がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ103は、アクセス経路情報テーブル1202を検索し、特定されたSCSIターゲットへ割り当てられている物理ポートのうち、IPSec機能を持つ物理ポートのオブジェクトID、IPアドレス及びTCPポート番号を特定する（ステップ2104）。

【0147】

その後、管理サーバ103は、ステップ2104で特定した情報、具体的には特定された物理ポートのオブジェクトID、IPアドレス及びTCPポート番号を、ディスカバリ要求を発行したサーバ101へ通知し、ステップ2101の処理に戻る（ステップ2105）。

【0148】

一方、ステップ2103においてディスカバリ要求を発行したサーバ101がIPSec機能を有する物理ポートを有しないと判断された場合、管理サーバ103は、アクセス経路情報テーブル1202を検索し、ディスカバリ要求を発行したサーバ101がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ103は、特定したSCSIターゲットに基づいてアクセス経路情報テーブル1202を検索し、特定されたSCSIターゲットへ割り当てられている物理ポートのうち、IPSec機能を持たない物理ポートのオブジェクトID、IPアドレス及びTCPポート番号を特定する（ステップ2106）。

【0149】

その後、管理サーバ103は、ステップ2206で特定した情報、具体的には特定された物理ポートのオブジェクトID、IPアドレス及びTCPポート番号を、ディスカバリ要求を発行したサーバ101へ通知し、ステップ2101の処理に戻る（ステップ2107）。

【0150】

第二の実施形態の他の変形例として、ディスカバリ要求を発行するサーバ101が、ディスカバリ要求にセキュリティレベルの要求（例えば暗号化の要否）を加える構成もある。このような構成にすることによって、サーバ101は、自身が要求するセキュリティレベルを満たすターゲットを管理サーバ103に要求することが出来る。

【0151】

このような構成は、例えば、iSNSプロトコルに用意された「Vendor Specific Attribute」及び「Vendor Specific Message」を利用することで可能になる。Vendor Specific Attributeは、iSNSサーバ（本実施形態では管理サーバ103）及びiSNSクライアント（本実施形態ではサーバ101や記憶装置システム102）に特定の属性を与えるために任意に使用可能なビット列を指す。又Vendor Specific Messageは、iSNSサーバとiSNSクライアント間で交換するパケット内に、任意の情報を埋め込んだものである。

【0152】

上述の「Vendor Specific Attribute」及び「Vendor Specific Message」を具体的には以下の様に利用する。Vendor Specific Attributeに登録する属性情報として「IPSec機能の有無」を定義する。具体的には、iSNSサーバが管理するポート毎、つまり、IPアドレス毎に、IPSecが使用可能であればビット列にビット1を、IPSecが使用不可能であればビット列にビット0を設定するように決める。また、「暗号化の要否」及び「IPSec機能の有無」の情報をやり取りするVendor Specific Messageを定義する。

【0153】

上述の定義において、iSNSクライアントがiSNSサーバへ自身のアドレスを登録する際、IPSec機能の使用可否の情報を埋め込んだ「IPSec機能の有無」メッセージをiSNSサーバに送信する。これにより、iSNSサーバは、iSNSクライアントの「IPSec機能の有無」に関する属性情報を収集することができる。その後iSNSクライアントは、iSNSサーバへディスカバリ要求を発行する際、暗号化が必要か否かの情報を埋め込んだ「暗号化の要否」メッセージをディスカバリ要求に含めてiSNSサーバへ送信する。ディスカバリ要求を受けとったiSNSサーバは、収集したiSNSクライアントの「IPSec機能の有無」属性情報を検索し、ディスカバリ要求で暗号化が必要とされていれば、iSNSクライアントがアクセス可能な記憶装置システム102のなかで、IPSec機能を持つものだけを通知することが可能となる。

【0154】

図22は、上記他の変形例において、サーバ101がセキュリティレベル（ここでは暗号化の要否）を含めてディスカバリ要求を発行する際のネーム問い合わせ処理の手順を示す図である。ディスカバリ要求に基づいた処理を行っていない場合、管理サーバ103は

サーバ101からディスクバリ要求を受信したかどうかを監視している（ステップ2201）。

【0155】

ディスクバリ要求を受け取った管理サーバ103は、受信したディスクバリ要求に含まれる情報に基づいて、ディスクバリ要求を発行したサーバ101が暗号化を必要としているかの判定を行う（ステップ2202）。

【0156】

ディスクバリ要求を発行したサーバ101が暗号化を必要としていると判断された場合、管理サーバ103は、上述した変形例（図21）におけるステップ2104及び2105と同様の処理を行う。具体的には、管理サーバ103は、サーバ101がアクセス可能なSCSIターゲットのうち、IPSec機能を有する物理ポートを有するSCSIターゲットの情報をサーバ101へ送信する（ステップ2203及び2204）。

【0157】

一方、ディスクバリ要求を発行したサーバ101が暗号化を必要としていないと判断された場合、管理サーバ103は、上述した変形例（図21）におけるステップ2106及び2107と同様の処理を行う。具体的には、管理サーバ103は、サーバ101がアクセス可能なSCSIターゲットのうち、IPSec機能を有さない物理ポートを有するSCSIターゲットの情報をサーバ101へ送信する（ステップ2205及び2206）。

【0158】

尚、ステップ2205において、管理サーバ103は、IPSecの機能の有無を判断する処理を省略し、単にサーバ101がアクセス可能なSCSIターゲットに割り当てられている物理ポートの情報をサーバ101へ送信しても構わない。つまり、サーバ101から低いセキュリティレベルの要求があった場合には、管理サーバ103は、低いセキュリティレベルに対応するSCSIターゲットの物理ポートでも、よりセキュリティレベルが高い物理ポートの情報をサーバに通知しても構わない。

【0159】

尚、第一の実施形態においても、管理サーバ103は第二の実施形態と同様に、記憶装置システム102に対して一つのボリュームに対して複数の物理ポート125を割り当てるように指示することが出来る。この場合、ボリューム作成完了をサーバ101に通知する際に、管理サーバ103は、一つのボリュームに割り当てた複数の物理ポート125に関する情報も併せて通知する。通知を受けたサーバ101は、サーバ101で定めた任意の条件（例えば通知された一方の物理ポート125のみを通常使用し、もう一方の物理ポート125を代替パス用とする等）に基づいて通知された物理ポート125を使用する。

【0160】

この場合、サーバ101に通知される複数の物理ポートの情報は、双方ともセキュリティレベルが高い物理ポートでも、一部のみセキュリティレベルが高い物理ポートでも、全てセキュリティレベルが低い物理ポートの情報でも良い。例えば、サーバ101からの要求が高いセキュリティレベルである場合には、全て高いセキュリティレベルの物理ポートに関する情報が通知される場合や、少なくとも一つの高いセキュリティレベルの物理ポートに関する情報が含まれる場合もある。

【0161】

第二の実施形態では、管理サーバ103は、ディスクバリ要求を受信した際、サーバ101がアクセス可能なボリュームに割り当てられている物理ポートを任意に（あるいはサーバ101の物理ポートの種類もしくはサーバ101からのセキュリティレベルに応じて）選択し、その選択された物理ポートの情報をサーバ101へ送信していた。しかし、第二の実施形態のようにすると、サーバ101自身でボリュームへのアクセスについてのセキュリティレベルを随時変更することが難しい。

【0162】

そこで、第3の実施形態として、サーバ101自身がセキュリティレベルに応じてボリュームへアクセスする物理ポートを選択する構成を考える。

具体的には、管理サーバ 1 0 3 が、サーバ 1 0 1 からのディスクバリ要求に対し、サーバ 1 0 1 がアクセス可能なボリュームに割り当てられている全ての物理ポートのオブジェクト ID、IP アドレス、TCP ポート番号及び IPSec 機能の有無の情報をサーバ 1 0 1 へ送信する構成とする。

【0 1 6 3】

更に、上述の情報を受信したサーバ 1 0 1 は、それらの情報をパス情報テーブル 1 1 1 に格納する。そして、サーバ 1 0 1 は、パス情報テーブル 1 1 1 に格納されているボリュームに対する複数の経路情報を元にして、IPSec による暗号化が必要な場合のみ IPSec 機能を持つ物理ポートを選択してアクセスするという構成とする。

【0 1 6 4】

図 2 3 は、本実施形態におけるパス情報テーブル 1 1 1 の構成例を示す図である。本実施形態におけるパス情報テーブルは、第一の実施形態で説明したパス情報テーブル 1 1 1 (図 4) の構成と基本的に同一である。しかし、図 4 で示したパス情報テーブル 1 1 1 とは、デバイス名に割り当てられた IP アドレスが複数の場合がある点及びこれらの IP アドレスに対応する物理ポートの IPSec 機能の有無の情報を登録するフィールド 2 3 0 6 を有する点異なる。

【0 1 6 5】

例えば、図 2 3 では、デバイス名が/dev/hdaのデバイスへは IP アドレス 10.10.10.201、TCP ポート番号 3260 のポートと、IP アドレス 10.10.10.202、TCP ポート番号 3 2 6 0 のポートが割り当てられている。IP アドレス 10.10.10.201、TCP ポート番号 3260 のポートは IPSec 機能を持つ物理ポートであり、IP アドレス 10.10.10.202、TCP ポート番号 3 2 6 0 のポートは IPSec 機能を持たない物理ポートである。

【0 1 6 6】

図 2 4 は、本実施形態において、サーバ 1 0 1 がパス管理プログラム 1 1 0 を実行することで行うパス選択処理の手順例を示した図である。サーバ 1 0 1 は、ボリュームへのアクセス要求に暗号化が必要である場合には IPSec を用いた通信経路を使用し、そうでない場合は、IPSec を使用しない通信経路を使用する。

【0 1 6 7】

まずサーバ 1 0 1 は、サーバ 1 0 1 自身で実行されているプログラムにおいて、ボリュームへのアクセス要求が発行されたか否かの判定を行う (ステップ 2 4 0 1)。

ボリュームへのアクセス要求が発行された場合、サーバ 1 0 1 は、パス情報テーブル 1 3 0 7 を検索し、アクセス要求の対象となるボリュームの情報が存在するかを確認する (ステップ 2 4 0 2、2 4 0 3)。

【0 1 6 8】

アクセス要求の対象となるボリュームの情報が存在しなかった場合、サーバ 1 0 1 は、管理サーバ 1 0 3 へのディスクバリ要求を発行する。ディスクバリ要求を受けた管理サーバ 1 0 3 は、図 2 2 に示した処理と同様のネーム問い合わせ処理を行う。

【0 1 6 9】

ステップ 2 4 0 3 でアクセス対象となるボリュームの情報が存在する場合又はステップ 2 4 0 4 の処理で管理サーバ 1 0 3 からアクセス対象となるボリュームの情報を取得した場合、サーバ 1 0 1 は、アクセス対象となるボリュームに対してアクセス経路が複数あるか否か判定する (ステップ 2 4 0 5)。

【0 1 7 0】

複数経路が存在する場合、サーバ 1 0 1 は、ボリュームへのアクセス要求を発行したプログラムが暗号化通信を必要としているか否かの判定を行う。この判定を行う方法として、例えば、ボリュームへのアクセスを行うプログラムが、アクセス要求へ暗号化の要否を含め、それをサーバ 1 0 1 が検出する方法や、サーバ 1 0 1 の使用者が、プログラム毎に暗号化の要否を事前に設定しておき、その設定に従って判定を行う方法などが考えられる (ステップ 2 4 0 6)。

【0 1 7 1】

プログラムが暗号化通信を必要としている場合、サーバ101は、複数あるアクセス経路のうち、ターゲット側でIPSec機能を持つ物理ポートが使用されるアクセス経路を選択する。そして、サーバ101は、選択したアクセス経路を用いて、アクセス対象となるボリュームを有する記憶装置システム102と通信を行う（ステップ2409）。

【0172】

一方、プログラムが暗号化通信を必要としない場合、サーバ101は、複数あるアクセス経路のうち、ターゲット側でIPSec機能を持たない物理ポートが使用されるアクセス経路を選択する。そして、サーバ101は、選択したアクセス経路を用いて、アクセス対象となるボリュームを有する記憶装置システム12と通信を行う（ステップ2408）。

【0173】

又、ステップ2405でアクセス経路が複数無いと判定された場合、サーバ101は、アクセス対象であるボリュームに対する唯一のアクセス経路を用いて記憶装置システム102と通信を行う。

【0174】

尚、第一の実施形態においても、第三の実施形態と同様のことを行うことができる。この場合、サーバ101は、ボリューム作成完了通知を受信する際に、複数のアクセス経路に関する情報を受け取り、パス情報テーブルへ登録する。

【図面の簡単な説明】

【0175】

【図1】 第一の実施形態におけるシステム構成例を示す図である。

【図2】 ポート情報テーブルの構成例を示す図である。

【図3】 ストレージ容量テーブルの構成例を示す図である。

【図4】 パス情報テーブルの構成例を示す図である。

【図5】 ボリューム情報テーブルの構成例を示す図である。

【図6】 パスワード管理テーブルの構成例を示す図である。

【図7】 ボリューム割り当て処理の手順例を示す図である。

【図8】 構成情報管理処理の手順例を示す図である。

【図9】 ボリューム作成と割り当て処理の手順例を示す図である。

【図10】 ボリューム作成と割り当て処理の手順例を示す図である。

【図11】 IPSecアカウント処理の手順例を示す図である。

【図12】 実施形態2におけるシステム構成例を示す図である。

【図13】 アクセス経路情報テーブルの構成例を示す図である。

【図14】 実施形態2におけるボリューム割り当て処理全体の手順例を示す図である。

【図15】 実施形態2におけるボリューム作成と割り当て処理の手順を示す図である。

【図16】 実施形態2におけるボリューム作成と割り当て処理の手順を示す図である。

【図17】 アクセス経路通知処理の手順を示す図である。

【図18】 ネーム問い合わせ処理の手順を示す図である。

【図19】 ボリューム情報テーブルの構成例を示す図である。

【図20】 アクセス経路情報テーブルの構成例を示す図である。

【図21】 ネーム問い合わせ処理の手順例を示す図である。

【図22】 ネーム問い合わせ処理の手順例を示す図である。

【図23】 パス情報テーブルの構成例を示す図である。

【図24】 パス選択処理の手順例を示す図である。

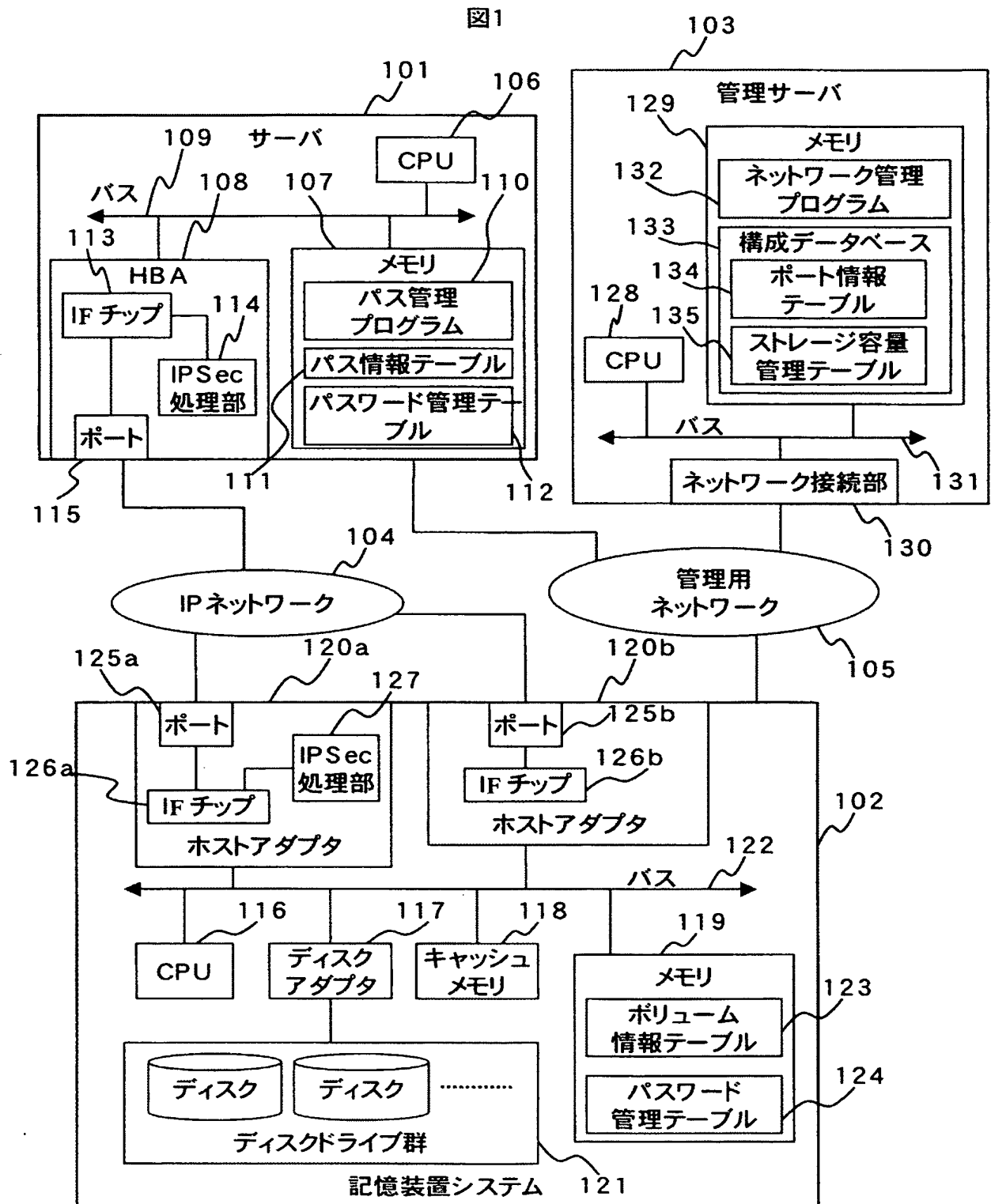
【符号の説明】

【0176】

101…サーバ、102…記憶装置システム、103…管理サーバ、104…IPネットワ

ーク、1 0 5…管理用ネットワーク。

【書類名】 図面
【図 1】



【図 2】

図2

装置 ID	オブジェクトID	IP アドレス	ノード 種別	IPSec 機能の 有無	認証 ID	パス ワード
Host 1	iqn.2003- 01.com.exampleホ st1	10.10.10. 101	ホスト	有り	10.10.1 0.101	aaaaaa
Host 2	iqn.2003- 02.com.exampleホ st2	10.10.10. 102	ホスト	無し	-	-
Host 3	iqn.2003- 03.com.exampleホ st3	10.10.10. 103	ホスト	有り	10.10.1 0.103	cccccc
Stora ge 1	iqn.2003- 03.com.example st orage 1	10.10.10. 201	ストレ ージ	有り	10.10.1 0.201	dddddd
	iqn.2003- 04.com.example st orage 1	10.10.10. 202	ストレ ージ	無し	-	-
Stora ge 2	iqn.2003- 05.com.example st orage 2	10.10.10. 203	ストレ ージ	有り	10.10.1 0.203	ffffff
	-	10.10.10. 204	ストレ ージ	無し	-	-
Stora ge 3	iqn.2003- 06.com.example st orage 3	10.10.10. 205	ストレ ージ	有り	10.10.1 0.205	hhhhhh

【図 3】

図3

装置ID	空き容量	使用容量
Storage 1	10TB	5TB
Storage 2	20TB	12TB
Storage 3	8TB	2TB

【図 4】

図4

デバイス名	オブジェクトID	LUN	IPアドレス	TCP ポート番号
/dev/sda	iqn.2003-03.com.example storage 1	0	10.10.10.201	3260
/dev/sdb		1		
/dev/sdc	iqn.2003-05.com.example storage 2	0	10.10.10.203	3261
/dev/sdd		1		

【図 5】

図5

物理 ボリューム 番号	LUN	容量	割り当てポートのIPアドレス	TCP ポート 番号	割り当てポート のオブジェクトID	IPSec 機能の 有無
Vol. 0	0	200GB	10.10.10.201	3260	iqn.2003-01.com.example storage 1	有り
Vol. 1	1	400GB				
Vol. 2	2	350GB				
Vol. 3	3	600GB	10.10.10.202	3261	iqn.2003-04.com.example storage 1	無し

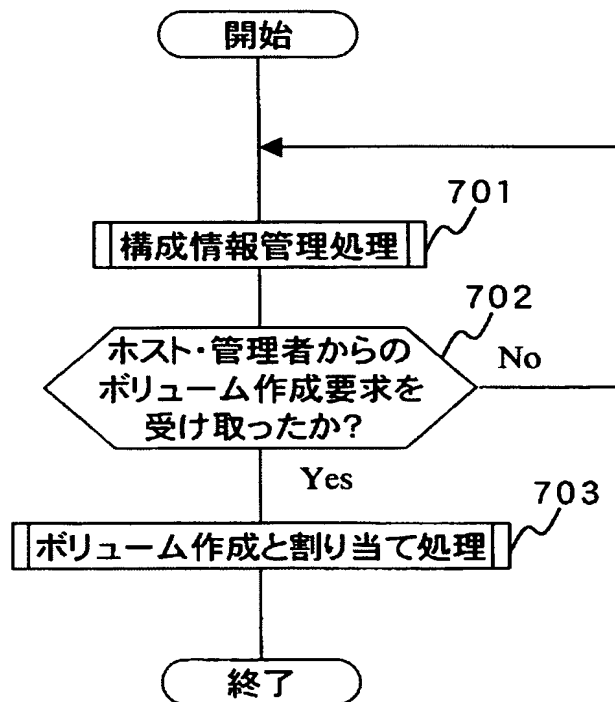
【図 6】

図6

認証ID	パスワード
10.10.10.201	dddddd
10.10.10.202	eeeeee

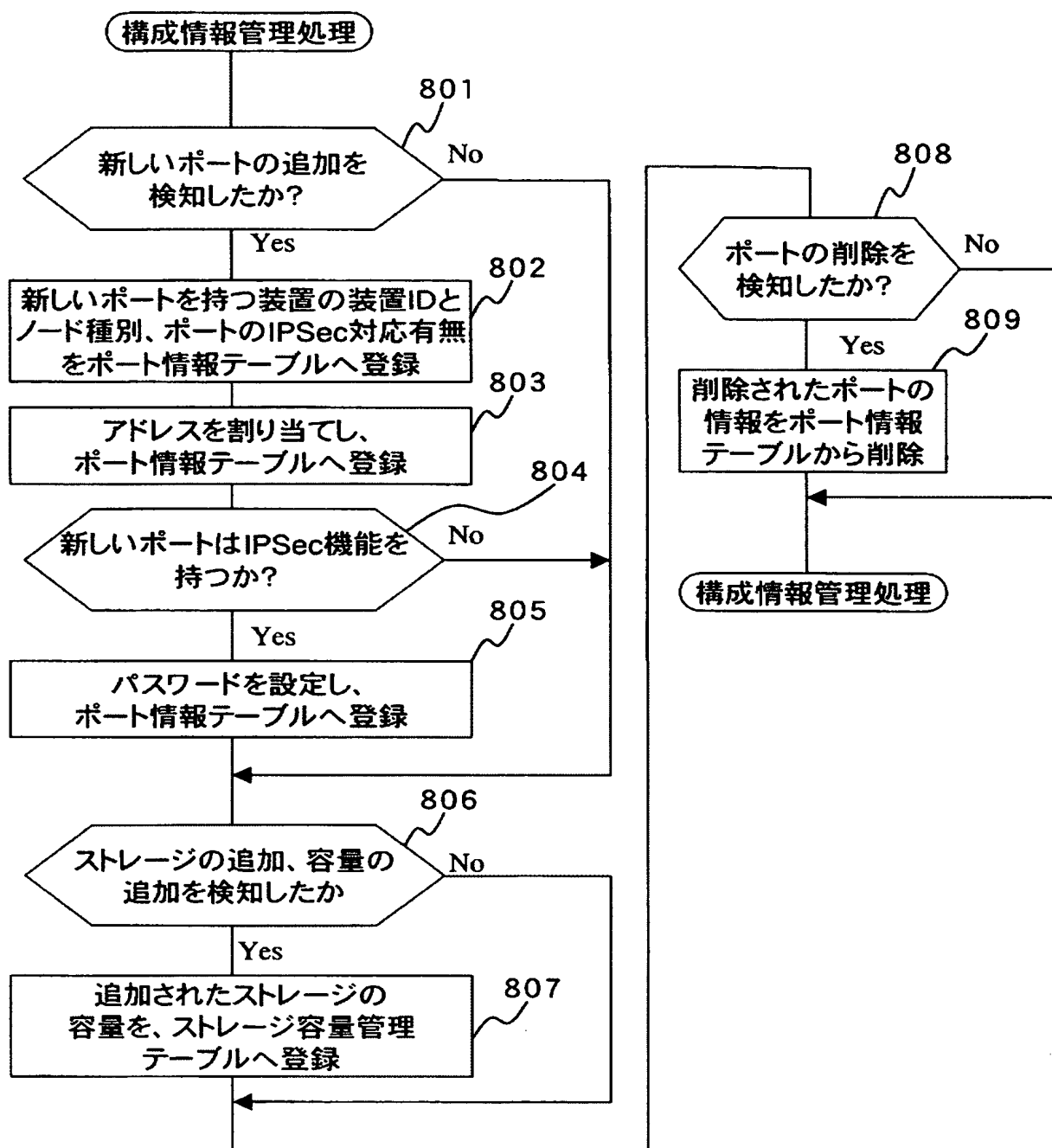
【図 7】

図7



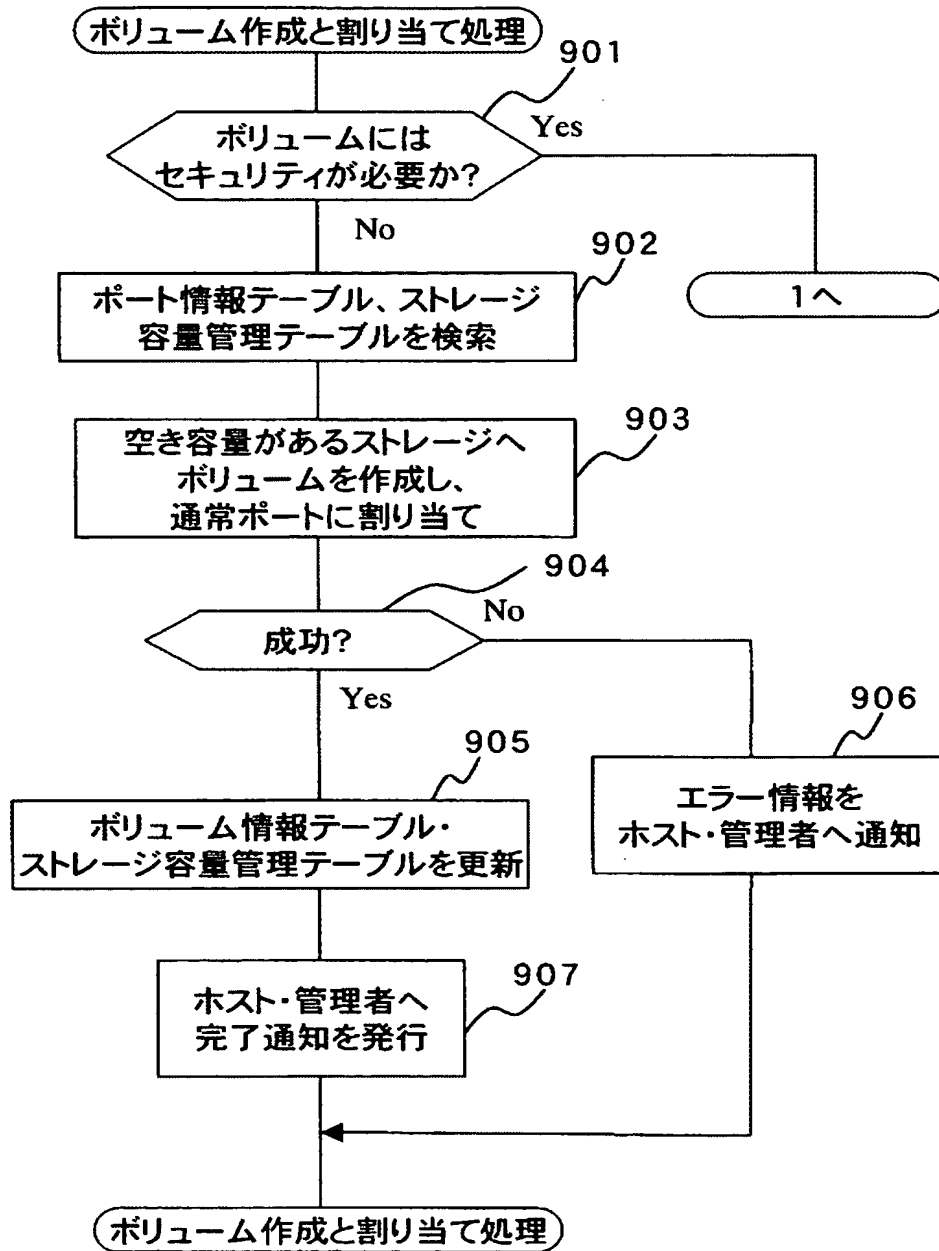
【図8】

図8



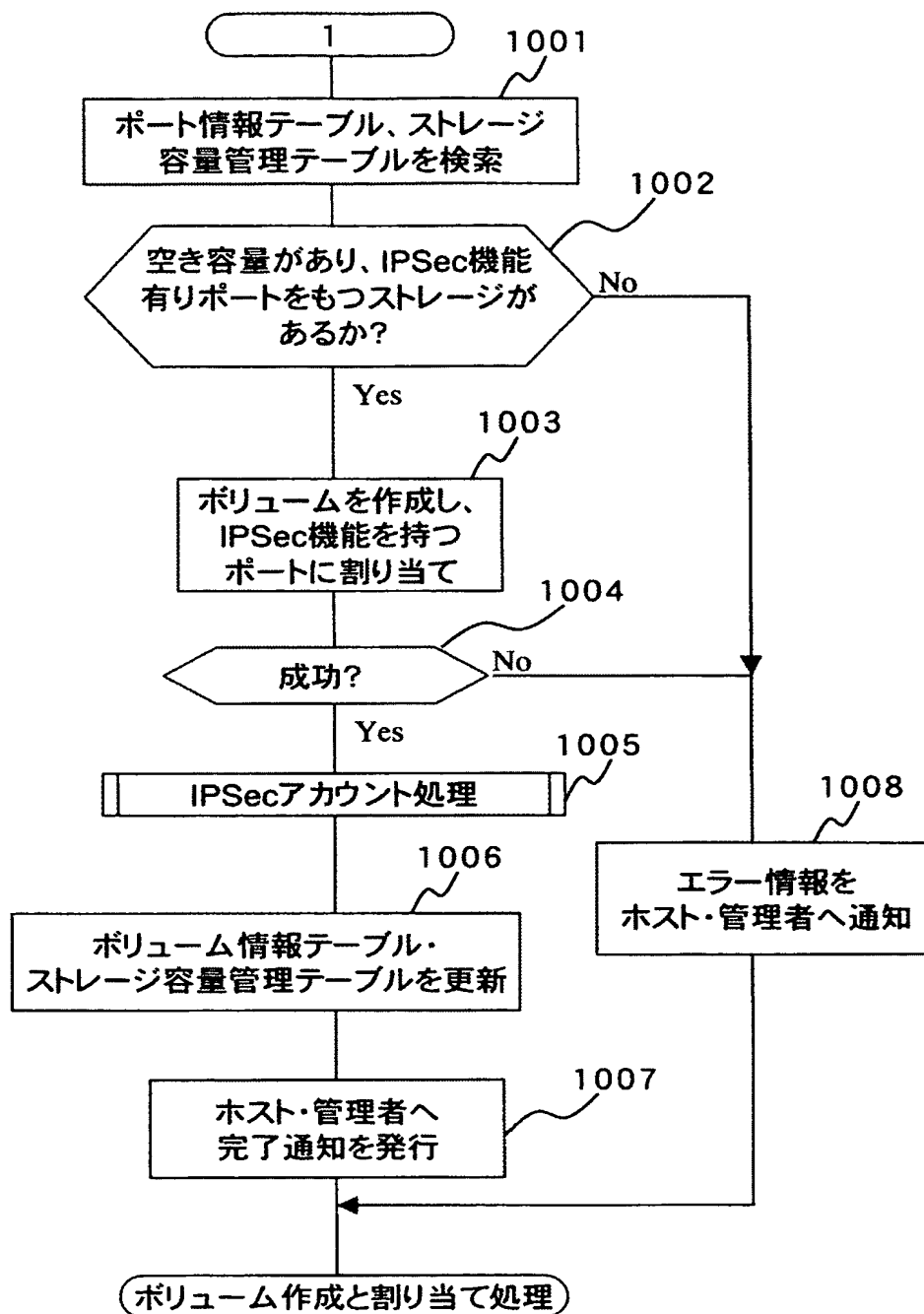
【図9】

図9



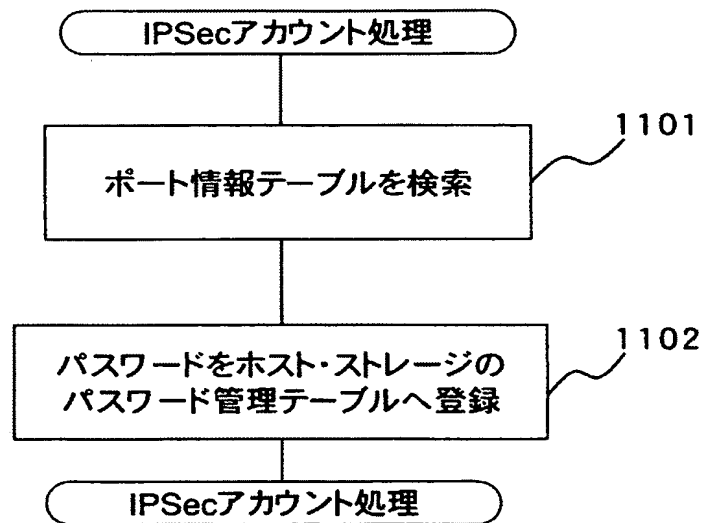
【図10】

図10



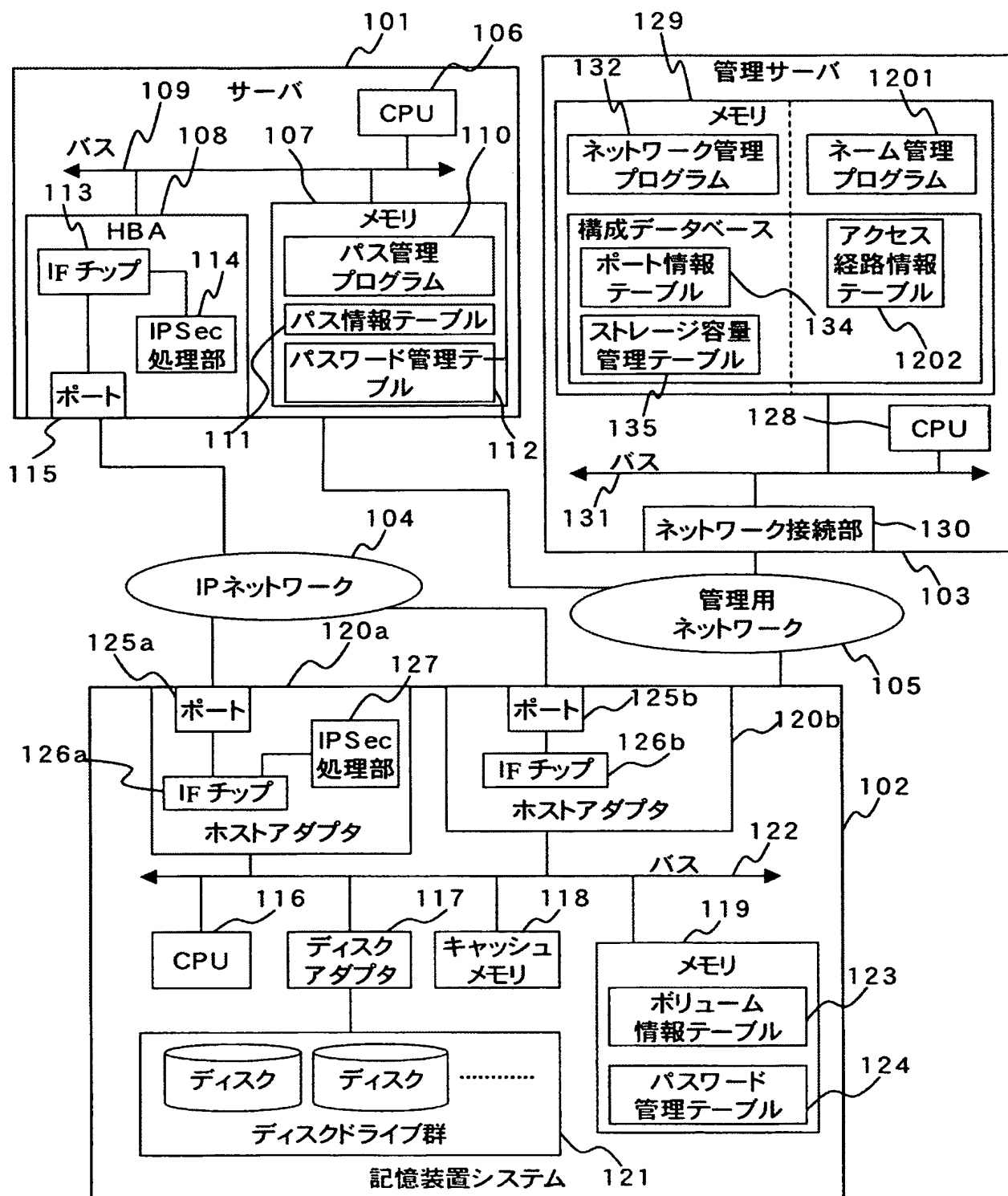
【図 11】

図11



【図12】

図12



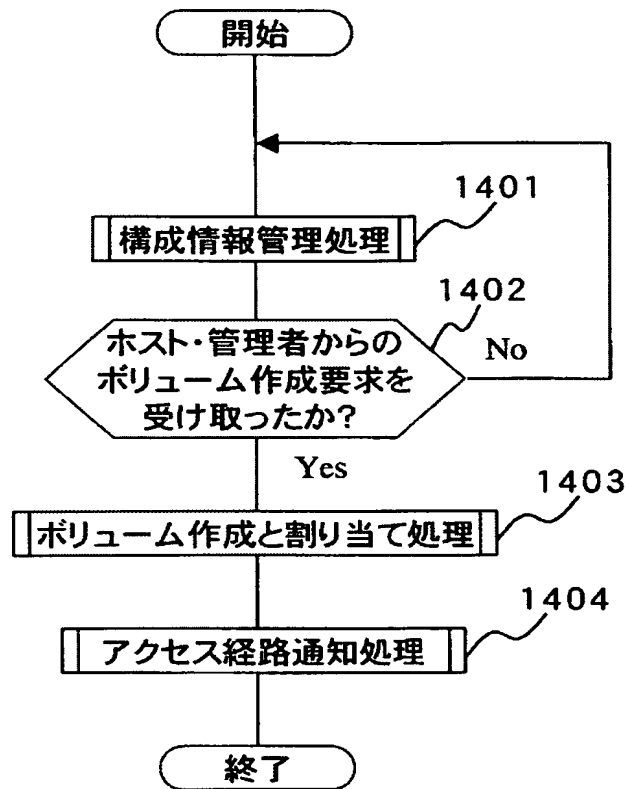
【図 13】

図13

オブジェクトID	IPアドレス	TCPポート番号	アクセス可能なホストのオブジェクトID
iqn.2003-03.com.example storage 1	10.10.10.201	3260	iqn.2003-01.com.example host1
			iqn.2003-02.com.example host2
iqn.2003-04.com.example storage 1	10.10.10.202	3261	iqn.2003-01.com.example host1
			iqn.2003-02.com.example host2
iqn.2003-05.com.example storage 2	10.10.10.203	3261	iqn.2003-01.com.example host1
iqn.2003-06.com.example storage 3	10.10.10.204	3260	iqn.2003-02.com.example host2

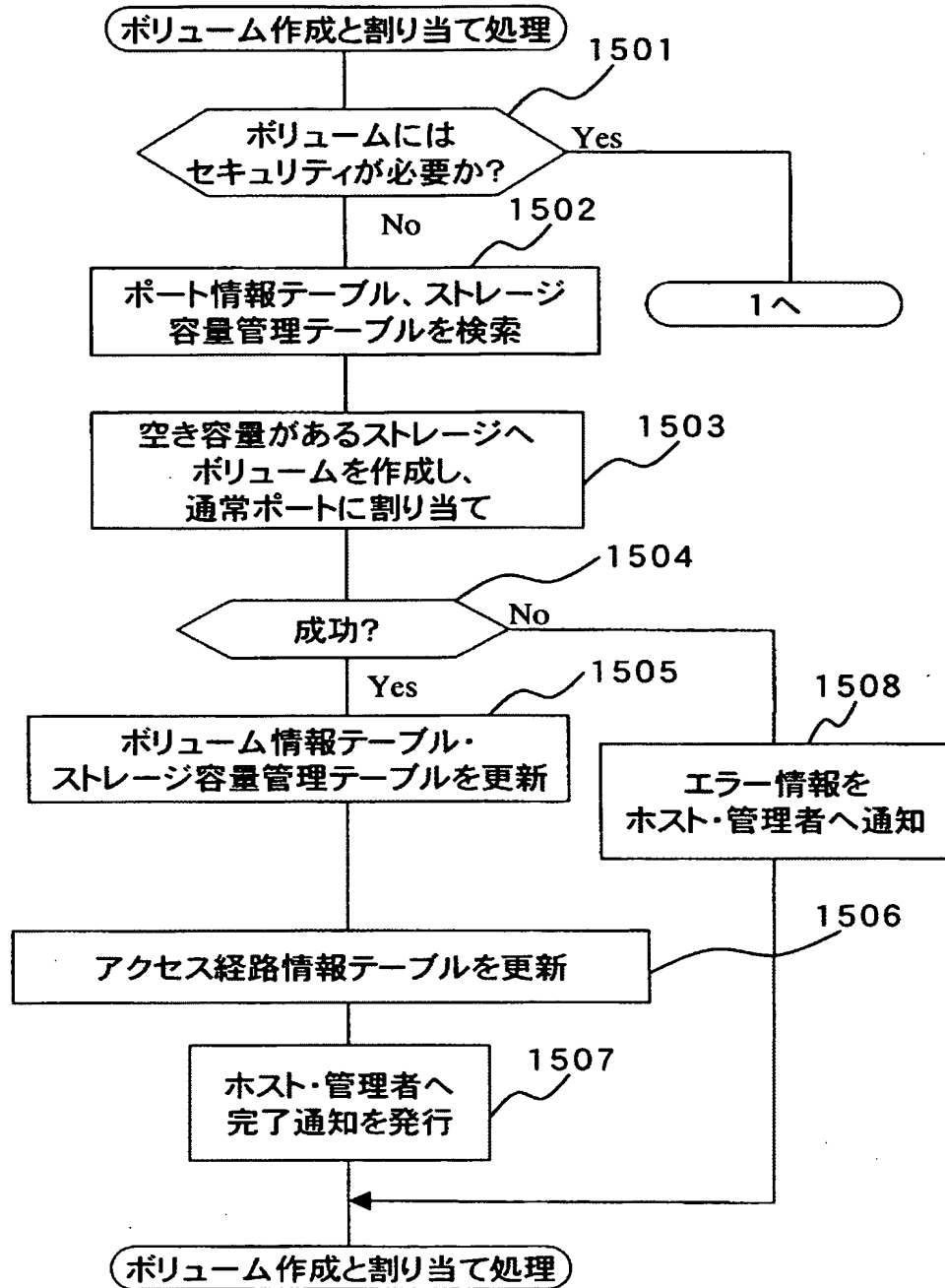
【図 14】

図14



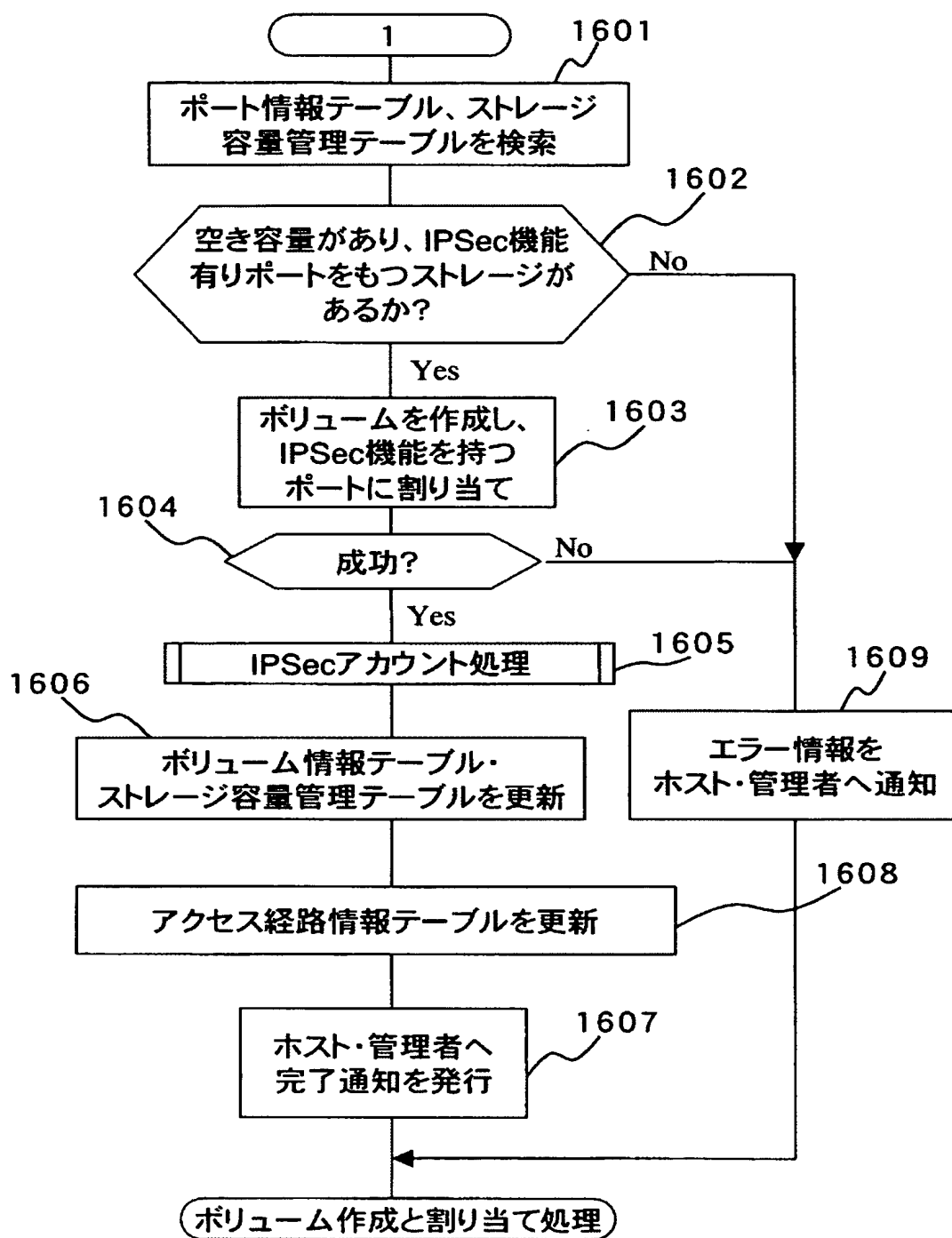
【図15】

図15



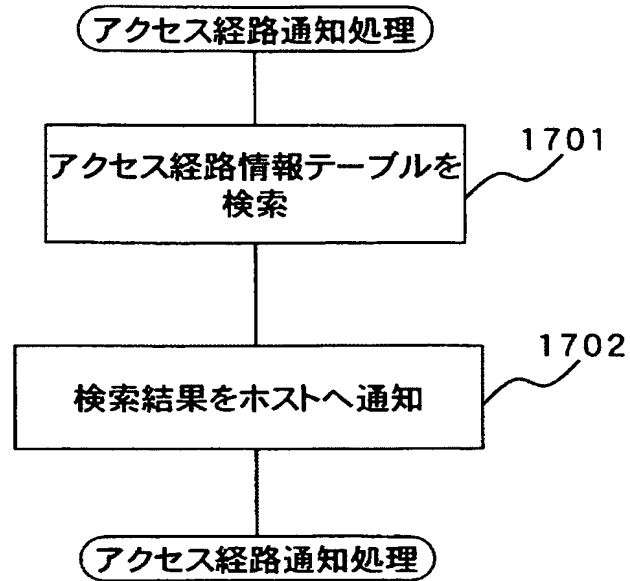
【図16】

図16



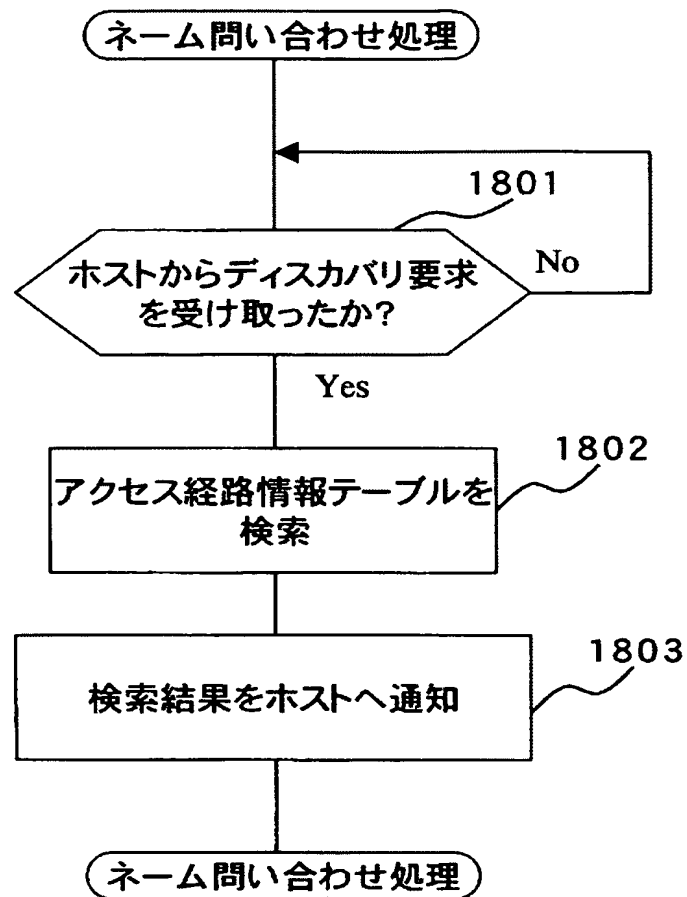
【図 17】

図17



【図18】

図18



【図 19】

図19

1901 物理 ボリューム 番号	1902 LUN	1903 容量	1904 割り当てポート のIPアドレス	1905 TCP ポート 番号	1906 割り当てポート のオブジェ クトID	1907 IPSec 機能の 有無
Vol. 0	0	200GB	10.10.10.201	3260	iqn.2003- 01.com.exam ple storage 1	有り
			10.10.10.202	3260		無し
Vol. 1	1	350GB	10.10.10.201	3260		有り
			10.10.10.202	3260		無し
Vol. 2	2	600GB	10.10.10.203	3261	iqn.2003- 02.com.exam ple storage 1	無し
			10.10.10.204	3260		有り
Vol. 3	3	400GB	10.10.10.203	3261		無し
			10.10.10.204	3260		有り

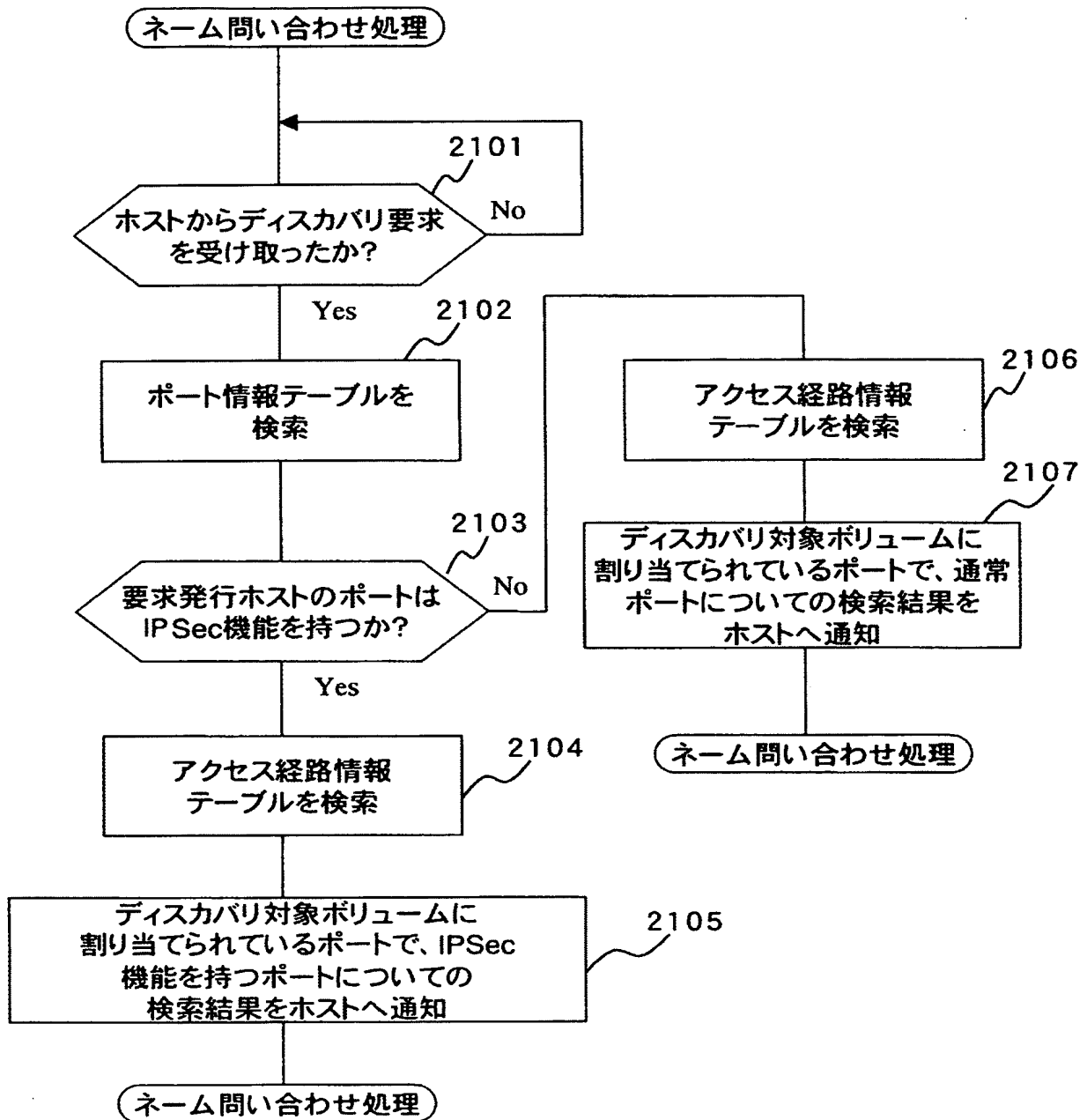
【図 20】

図20

2001 割り当てポートの オブジェクトID	2002 割り当てポート のIPアドレス	2003 TCPポ ート 番号	2004 IPSec 機能の 有無	2005 アクセス可能なホスト のオブジェクトID
iqn.2003- 01.com.example sto rage 1	10.10.10.201	3260	無し	iqn.2003- 01.com.example host1
	10.10.10.202	3260	有り	iqn.2003- 02.com.example host2
iqn.2003- 02.com.example sto rage 1	10.10.10.203	3261	無し	iqn.2003- 01.com.example host1
	10.10.10.204	3260	有り	iqn.2003- 02.com.example host2
iqn.2003- 03.com.example sto rage 2	10.10.10.205	3261	有り	iqn.2003- 01.com.example host1

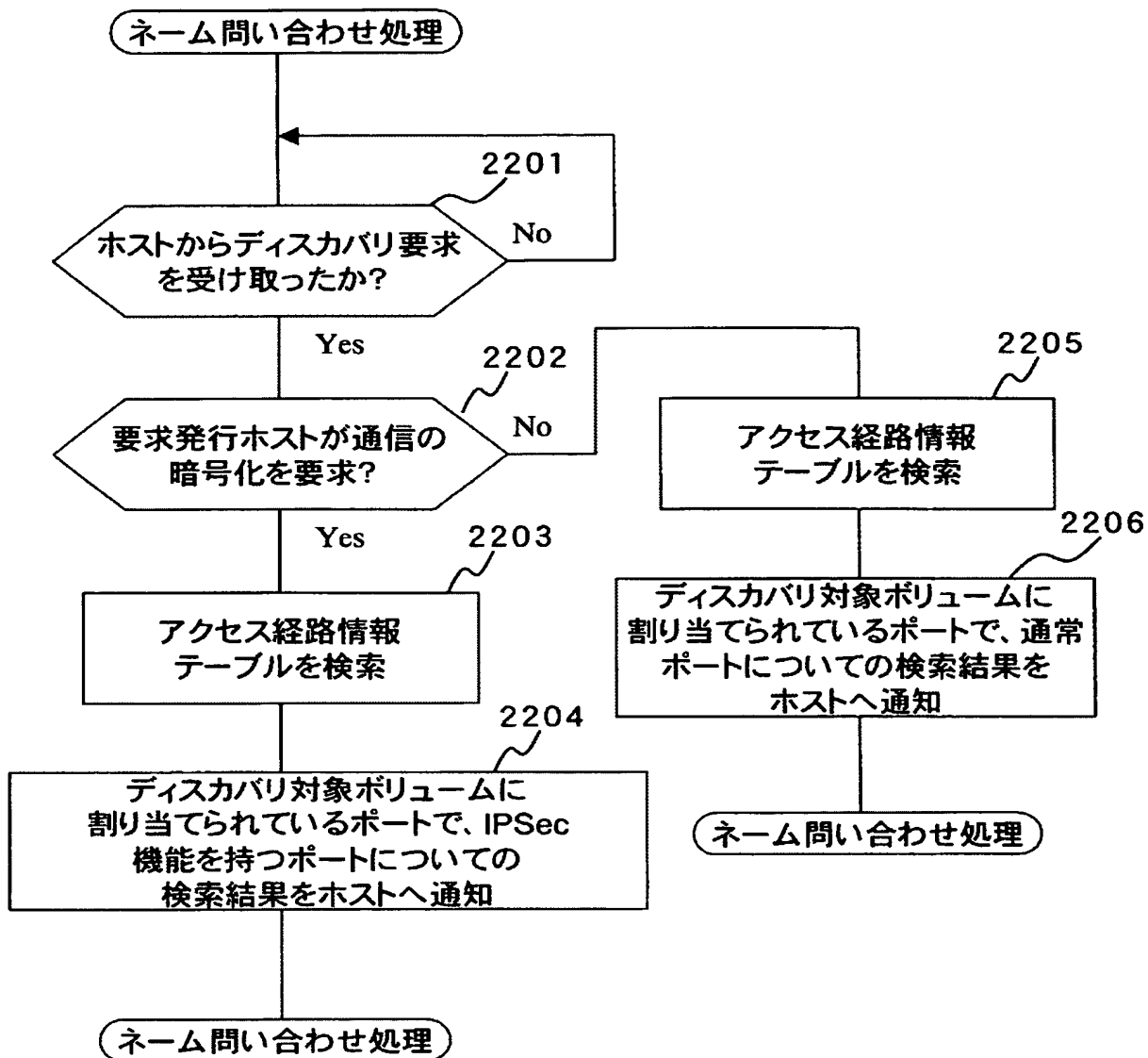
【図 21】

図21



【図 22】

図22



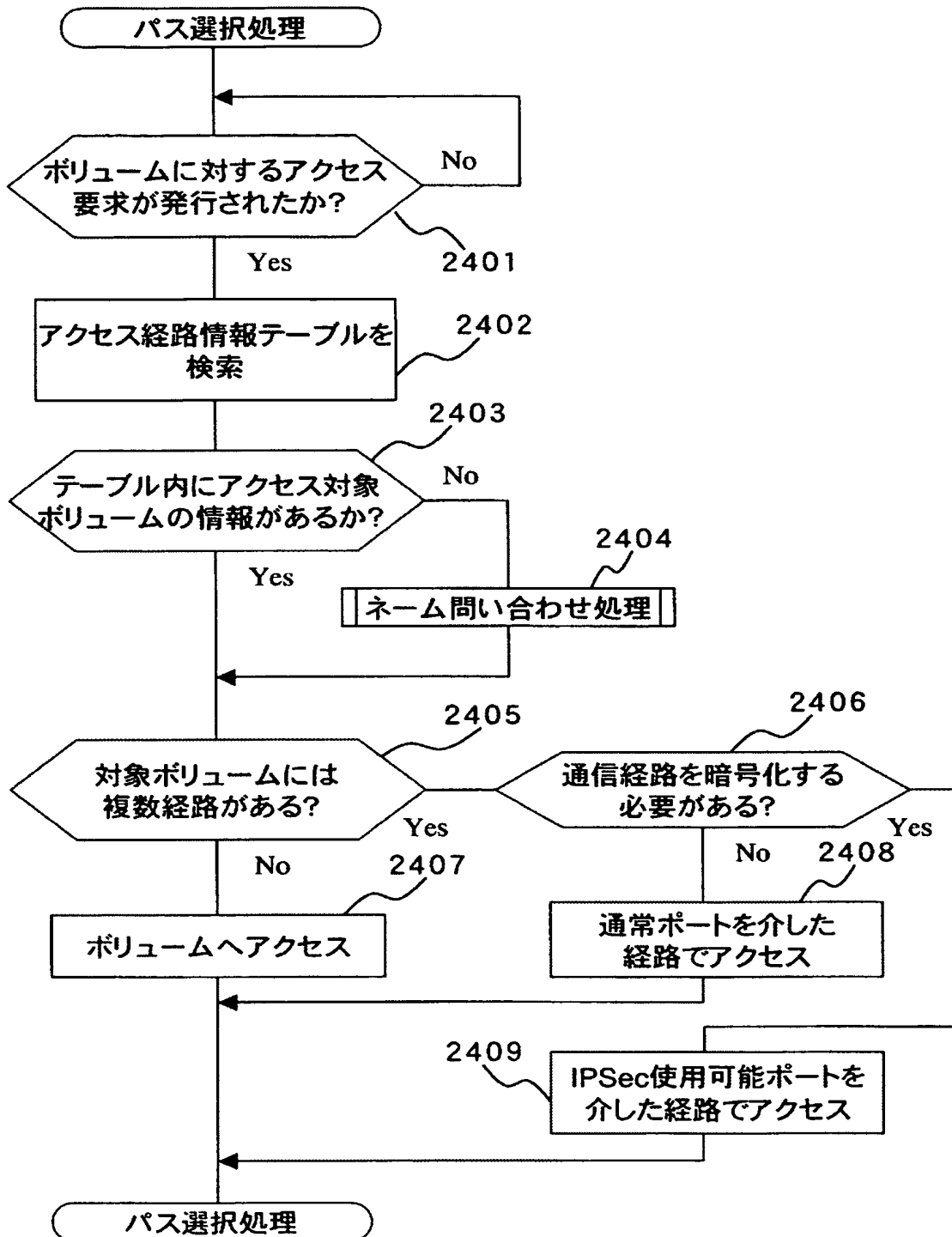
【図 23】

図23

2301 デバイス名	2302 オブジェクトID	2303 LUN	2304 IPアドレス	2305 TCP ポート 番号	2306 IPSec 機能の 有無
/dev/sda	iqn.2003-01.com.example:storage1	0	10.10.10.201	3260	無し
			10.10.10.202	3260	有り
/dev/sdb	iqn.2003-02.com.example:storage1	2	10.10.10.203	3261	無し
			10.10.10.204	3260	有り
/dev/sdc	iqn.2003-03.com.example:storage2	1	10.10.10.205	3261	有り

【図 24】

図24



【書類名】 要約書

【要約】

【課題】

セキュアな通信を行いたいボリュームへ、IPSec使用可能なポートを割り当てる作業を自動化できない。

【解決手段】

管理サーバが、物理ポートが持つセキュリティ機能の有無を管理し、その情報を元にボリューム作成後物理ポートへボリュームを割り当てるかを自動的に決定し、割り当て作業を行う。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 4 - 0 5 2 7 0 0
受付番号	5 0 4 0 0 3 1 7 9 5 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 6 年 3 月 1 日

< 認定情報・付加情報 >

【提出日】 平成16年 2月27日

特願 2 0 0 4 - 0 5 2 7 0 0

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所